Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

T.807

(05/2006)

SÉRIE T: TERMINAUX DES SERVICES TÉLÉMATIQUES

Technologies de l'information – Système de codage d'images JPEG 2000: système JPEG 2000 sécurisé

Recommandation UIT-T T.807

NORME INTERNATIONALE ISO/CEI 15444-8
RECOMMANDATION UIT-T T.807

Technologies de l'information – Système de codage d'images JPEG 2000: système JPEG 2000 sécurisé

Résumé

L'objectif de la présente Recommandation | Norme internationale est d'offrir une syntaxe permettant d'appliquer des services de sécurité aux données d'image à codage JPEG 2000. Ces services de sécurité comprennent la confidentialité, la vérification de l'intégrité, l'authentification de la source, l'accès conditionnel, le flux direct à échelonnement sécurisé et le transcodage sécurisé. La syntaxe permet d'appliquer, partiellement ou totalement, ces services de sécurité à des données d'image codées ou non codées, conservant ainsi les caractéristiques intrinsèques du codage JPEG 2000, comme l'échelonnabilité et l'accès à une diversité de zones spatiales, de niveaux de résolution, de composantes chromatiques et de couches qualitatives tout en apportant des services de sécurité à ces éléments.

Source

La Recommandation UIT-T T.807 a été approuvée le 29 mai 2006 par la Commission d'études 16 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8. Un texte identique est publié comme Norme Internationale ISO/CEI 15444-8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

A "l'ère numérique", le réseau Internet offre aux ayants droit de nombreuses et nouvelles opportunités concernant la distribution électronique de leurs œuvres (livres, films, partitions musicales, images, etc.).

En même temps, de nouvelles technologies de l'information simplifient radicalement l'accès aux contenus par les utilisateurs. Cela va de pair avec le problème généralisé des copies numériques piratées – avec la même qualité que l'original – et avec celui du "partage de fichiers" dans les réseaux d'homologue à homologue, ce qui engendre des plaintes récurrentes, concernant de grandes pertes, de la part de l'industrie des contenus.

L'Organisation mondiale de la propriété intellectuelle (OMPI) et ses (170) pays Membres ont un important rôle à jouer afin de garantir que le droit d'auteur, ainsi que l'expression culturelle et intellectuelle qu'il suscite, restera bien protégé au cours du 21e siècle. La nouvelle économie numérique et les créateurs de chaque pays du monde en dépendent. C'est pourquoi, en décembre 1996, le Traité de l'OMPI sur le droit d'auteur (WCT) a été promulgué avec deux importants articles (11 et 12) sur les obligations relatives aux mesures techniques et aux informations sur le régime des droits:

Article 11

Obligations relatives aux mesures techniques

Les Parties contractantes doivent prévoir une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits en vertu du présent traité ou de la Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs œuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi.

Article 12

Obligations relatives aux informations sur le régime des droits

(1) Les Parties contractantes doivent prévoir des sanctions juridiques appropriées et efficaces contre toute personne qui accomplit l'un des actes suivants en sachant, ou, pour ce qui relève des sanctions civiles, en ayant des raisons valables de penser que cet acte va entraîner, permettre, faciliter ou dissimuler une atteinte à un droit prévu par le présent traité ou la Convention de Berne:

(i) supprimer ou modifier, sans y être habilitée, toute information relative au régime des droits se présentant sous forme électronique;

(ii) distribuer, importer aux fins de distribution, radiodiffuser ou communiquer au public, sans y être habilitée, des œuvres ou des exemplaires d'œuvres en sachant que des informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

(2) Dans le présent article, l'expression "les informations sur le régime des droits" s'entend des informations permettant d'identifier l'œuvre, l'auteur de l'œuvre, le titulaire de tout droit sur l'œuvre ou des informations sur les conditions et modalités d'utilisation de l'œuvre, et de tout numéro ou code représentant ces informations, lorsque l'un quelconque de ces éléments d'information est joint à l'exemplaire d'une œuvre ou apparaît en relation avec la communication d'une œuvre au public.

Ce traité fournit une base solide afin de protéger la propriété intellectuelle. En 2004, une cinquantaine de pays avaient ratifié cet important traité. L'on s'attend donc que les outils et méthodes de protection qui sont recommandés dans le système JPEG 2000 ne manqueront pas d'assurer la sécurité des transactions, la protection des contenus (droits de propriété intellectuelle (IPR, Intellectual Property Rights)) et la protection des technologies.

Les questions de sécurité telles que l'authentification, l'intégrité des données, la protection du droit d'auteur et de la propriété intellectuelle, la protection de la sphère privée, l'accès conditionnel, la confidentialité, le suivi des transactions, pour n'en mentionner que quelques-unes, font partie des caractéristiques importantes dans de nombreuses applications d'imagerie visées par le système JPEG 2000.

Les moyens techniques permettant de protéger un contenu numérique sont décrits et peuvent être réalisés par de nombreux procédés tels que le filigranage numérique, la signature numérique, le chiffrement, les données métalinguistiques (métadonnées), l'authentification et la vérification d'intégrité.

La présente Partie 8 de la norme JPEG 2000 vise à offrir des outils et des solutions en termes de spécifications permettant aux applications de produire, de consommer et d'échanger des flux à codage JPEG 2000 sécurisé. C'est ce qui est désigné par le terme de **syntaxe JPSEC**.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Système de codage d'images JPEG 2000: système JPEG 2000 sécurisé

1 Domaine d'application

La présente Recommandation | Norme internationale spécifie le cadre, les concepts et les méthodes permettant de sécuriser les flux à codage JPEG 2000. Le domaine d'application de la présente Recommandation | Norme internationale consiste à définir:

1) une syntaxe normative de flux codé contenant des informations permettant d'interpréter des données d'image sécurisées;
2) un processus normatif permettant d'enregistrer des outils JPSEC auprès d'un organisme d'enregistrement délivrant un identificateur unique;
3) des exemples informatifs d'outils JPSEC dans des cas de figure typiques;
4) des directives informatives sur la façon de mettre en œuvre des services de sécurité et les métadonnées associées.

Le domaine d'application de la présente Recommandation | Norme internationale ne vise pas à décrire des applications spécifiques d'imagerie sécurisée ni à limiter l'imagerie sécurisée à des techniques spécifiques, mais à créer un cadre autorisant de futures extensions au fur et à mesure de l'évolution des techniques d'imagerie sécurisée.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT (TSB) tient à jour une liste des Recommandations de l'UIT-T en vigueur.

– Recommandation UIT-T T.800 (2002) | ISO/CEI 15444-1:2004, *Technologies de l'information – Système de codage d'images JPEG 2000: Système de codage noyau*.

– Recommandation UIT-T T.801 (2002) | ISO/CEI 15444-2:2004, *Technologies de l'information – Système de codage d'images JPEG 2000: Extensions*.

3 Termes et définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent. Les définitions données dans la Rec. UIT-T T.800 | ISO/CEI 15444-1, § 3, s'appliquent à la présente Recommandation | Norme internationale.

3.1 **contrôle d'accès**: prévention d'un usage non autorisé d'une ressource, y compris la prévention de l'utilisation d'une ressource de façon non autorisée.

3.2 **authentification**: processus de vérification d'une identité revendiquée par ou pour une entité systémique.

3.2.1 **authentification de la source**: vérification du fait qu'une entité d'origine (p. ex. un utilisateur/correspondant) est réellement l'entité d'origine revendiquée.

3.2.2 **authentification d'image fragile/semi-fragile**: processus visant à la fois l'authentification d'image de la source et la vérification de l'intégrité des données ou du contenu d'image, qui devrait être en mesure de détecter toute

modification du signal et de déterminer où cette modification a eu lieu, en précisant éventuellement quelle était la nature du signal avant sa modification.

NOTE – Ce processus sert à prouver l'authenticité d'un document. La différence entre authentification fragile et authentification semi-fragile d'une image est que la première consiste à vérifier l'intégrité des données d'image et la seconde à vérifier l'intégrité du contenu d'image.

3.3 confidentialité: propriété par laquelle des informations ne sont pas mises à la disposition ni révélées à des individus, entités ou processus non autorisés.

3.4 découpage des données: méthode visant à protéger des données sensibles contre un accès non autorisé en chiffrant ces données et en mémorisant différentes portions du fichier dans différents serveurs distants.

NOTE – Quand des données découpées font l'objet d'un accès, les parties sont extraites, combinées et déchiffrées. Une personne non autorisée aurait besoin de connaître les emplacements des serveurs contenant les parties, d'être en mesure d'avoir accès à chaque serveur, de savoir quelles sont les données à combiner et de savoir comment les déchiffrer.

3.5 déchiffrement: transformation inverse du chiffrement

3.6 signature numérique: donnée adjointe à une unité de données – ou transformation cryptographique de cette unité – qui permet à un destinataire de cette unité de données d'en prouver l'origine et l'intégrité, et qui permet de la protéger contre une création frauduleuse, p. ex. par son destinataire.

3.7 chiffrement: transformation réversible de données par un algorithme cryptographique afin de produire un cryptogramme, c'est-à-dire afin de masquer le contenu informationnel des données.

NOTE – Un synonyme du terme *algorithme de chiffrement* est: *chiffre*.

3.8 empreinte digitale: caractéristique d'un objet qui tend à distinguer d'autres objets similaires afin de permettre à son propriétaire de retrouver la trace d'utilisateurs autorisés les distribuant illégalement.

NOTE – A cet égard, la prise d'empreintes digitales est habituellement analysée dans le contexte du problème de la recherche criminelle.

3.9 fonction de hachage: fonction qui fait correspondre des chaînes de bits à des chaînes de bits de longueur fixe en répondant aux deux conditions suivantes.

NOTE – Pour une sortie donnée, il est mathématiquement impossible de trouver une entrée qui mappe à cette sortie; pour une entrée donnée, il est mathématiquement impossible de trouver une seconde entrée qui mappe à la même sortie. La faisabilité mathématique dépend des exigences de sécurité propres à l'utilisateur et à son environnement.

3.10 intégrité: propriété d'être en mesure de sauvegarder la précision et la complétude de ressources.

3.10.1 intégrité des données d'image: propriété par laquelle des données n'ont pas été altérées ni détruites de façon non autorisée.

3.10.2 intégrité du contenu d'image: assurance que le contenu d'image n'a pas été modifié par des utilisateurs non autorisés au point de modifier la perception de sa signification.

NOTE – Cette propriété permet d'appliquer à l'image des opérations de protection du contenu sans déclencher l'alarme d'intégrité.

3.11 application JPSEC: tout processus logiciel ou matériel qui est capable de consommer des flux à codage JPSEC en interprétant la syntaxe JPSEC afin d'offrir les services de sécurité spécifiés.

NOTE – Une application JPSEC fait usage d'un ou de plusieurs outils JPSEC.

EXEMPLE – Une application JPSEC sera en mesure de lire des flux JPSEC codés et chiffrés, de les déchiffrer si la clé appropriée lui a été fournie et de restituer sans codage les données d'image JPEG 2000 originales.

3.12 flux à codage JPSEC: séquence de bits résultant du codage et de la sécurisation d'une image au moyen du codage JPEG 2000 et des outils de sécurité JPSEC.

3.12.1 créateur JPSEC: entité qui crée un flux à codage JPSEC à partir d'une image, d'un flux à codage JPEG 2000, ou d'un autre flux à codage JPSEC afin d'offrir certains services JPSEC.

3.12.2 consommateur JPSEC: entité qui reçoit un flux à codage JPSEC et qui rend un service JPSEC fondé sur le flux codé.

3.13 service JPSEC: service qui protège la consommation d'images à codage JPEG 2000. Ce service déjoue les attaques compromettant la sécurité et fait usage d'un ou de plusieurs outils JPSEC.

3.14 organisme d'enregistrement JPSEC: entité chargée de délivrer un identificateur unique afin de faire référence à un outil JPSEC et chargée de mémoriser la liste des paramètres contenus dans la description d'outil JPSEC.

3.15 outil JPSEC: processus matériel ou logiciel qui utilise des techniques de sécurité afin de mettre en œuvre un service de sécurité

3.15.1 outil JPSEC normatif: outil JPSEC qui utilise des modèles d'outil prédéfinis pour le déchiffrement, pour l'authentification ou pour le hachage comme spécifié par la partie normative de la présente Recommandation | Norme internationale.

3.15.2 outil JPSEC non normatif: outil JPSEC spécifié par un numéro d'identification attribué par l'organisme d'enregistrement JPSEC ou par une application définie par l'utilisateur.

3.15.3 outil JPSEC défini par l'utilisateur: outil JPSEC non normatif qui est défini par une application définie par l'utilisateur.

3.15.4 outil JPSEC défini par l'organisme d'enregistrement: outil JPSEC non normatif qui est défini par l'organisme d'enregistrement JPSEC.

3.16 description d'outil JPSEC: description des paramètres utilisés par l'outil JPSEC.

NOTE – La description d'outil JPSEC ne décrit toutefois pas l'algorithme ou la méthode que l'on utilise. Une description d'outil JPSEC se compose de deux parties: la liste des paramètres et ses valeurs. Dans le cas d'outils JPSEC normatifs, la liste des paramètres est donnée par la norme. Dans le cas d'outils JPSEC non normatifs, la liste des paramètres peut être fournie par l'organisme d'enregistrement. Dans les deux cas, les valeurs paramétriques sont spécifiées dans les segments marqueurs SEC et INSEC.

3.17 clé: séquence de symboles qui commande les opérations de chiffrement et de déchiffrement.

3.17.1 clés symétriques: paire de clés pour lesquelles aussi bien l'expéditeur que le destinataire utilisent la même clé secrète ou deux clés qui peuvent être facilement calculées, l'une à partir de l'autre, dans un système cryptographique.

3.17.2 paire de clés asymétriques: paire de clés associées où la clé privée définit la transformation privée et où la clé publique définit la transformation publique.

3.17.2.1 clé privée: clé faisant partie d'une paire de clés asymétriques d'entité, qui ne devrait pas être révélée.

3.17.2.2 clé publique: clé faisant partie d'une paire de clés asymétriques d'entité, qui peut être rendue publique.

3.18 production de clé, fonction de production de clé: fonction qui reçoit en entrée un certain nombre de paramètres dont au moins un doit être secret, et qui envoie en sortie des clés appropriées à l'algorithme et à l'application que l'on envisage.

NOTE – La fonction doit avoir la propriété qu'il doit être mathématiquement impossible de déduire la sortie sans connaissance préalable de l'entrée secrète.

3.19 gestion des clés: production, mémorisation, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.

3.20 émulation de marqueur: cryptogramme résultant du processus de chiffrement, qui contient un code de déclenchement JPEG.

3.21 algorithme d'un code d'authentification de message, fonction de contrôle cryptographique, fonction de somme de contrôle cryptographique: algorithme permettant de calculer une fonction qui affecte des chaînes de bits et une clé secrète à des chaînes de bits de longueur fixe, en satisfaisant les deux propriétés suivantes:

- pour toute clé et toute chaîne d'entrée, la fonction peut être calculée efficacement;
- pour toute clé fixe, sans aucune connaissance préalable de la clé, il est mathématiquement impossible de calculer la valeur de la fonction d'après une quelconque nouvelle chaîne d'entrée, même avec la connaissance de l'ensemble des chaînes d'entrée et des valeurs correspondantes de la fonction, où la valeur de la ième chaîne d'entrée peut avoir été choisie après observation de la valeur des i-1 premières valeurs de la fonction.

NOTE – La faisabilité mathématique dépend des exigences de sécurité propres à l'utilisateur et de son environnement.

3.21.1 code d'authentification de message (code MAC, *message authentication code*): chaîne de bits qui est la sortie d'un algorithme de codage MAC.

3.22 non-répudiation: association d'une entité à une transaction à laquelle elle participe, de façon que cette transaction ne puisse pas être ultérieurement répudiée (refusée).

NOTE – C'est-à-dire que le récepteur d'une transaction est en mesure de démontrer à une tierce partie neutre que l'expéditeur revendiqué a effectivement envoyé la transaction.

3.23 paquet: partie du flux de bits conforme à la Partie 1 de la norme JPEG 2000, composée d'un en-tête de paquet et des données d'image comprimées extraites d'une couche donnée du district d'une composante de pavé donnée, à une résolution donnée.

NOTE – Ce terme possède un acception différente du terme "paquet" qui est utilisé en transmission de données dans un réseau.

3.24 protection: processus visant à sécuriser un contenu.

3.24.1 modèle de protection: champs de modèle ou de liste de paramètres, nécessaires au fonctionnement d'une méthode de protection.

3.24.1 méthode de protection: méthode servant à créer ou à consommer un contenu protégé, telle que le chiffrement, le déchiffrement, l'authentification et la vérification d'intégrité.

3.25 sécurité: tous les aspects contribuant à définir, à réaliser et à conserver la confidentialité, l'intégrité, la disponibilité, l'imputabilité, l'authenticité et la fiabilité.

NOTE – Un produit, système ou service est considéré comme étant sécurisé si ses utilisateurs peuvent partir du principe qu'il fonctionne (ou va fonctionner) de la façon prévue. La sécurité est habituellement considérée dans le contexte d'une évaluation de dangers, réels ou perçus comme tels.

3.26 syntaxe de signalisation: spécification du format du flux à codage JPSEC qui contient toutes les informations requises pour consommer des images à codage JPEG 2000 sécurisé.

3.27 transcodage: opération consistant à recevoir en entrée un flux codé comprimé et à l'adapter ou à le convertir afin d'émettre en sortie un flux codé comprimé qui possède une certaine propriété recherchée.

EXEMPLE – Le flux codé comprimé de sortie peut représenter une image avec une résolution spatiale inférieure ou avec un débit binaire inférieur au flux codé comprimé d'entrée.

3.27.1 transcodage sécurisé: opération consistant à exécuter le transcodage ou l'adaptation d'une entrée de contenu comprimé protégé sans compromettre cette protection.

NOTE – Le terme *transcodage sécurisé* est utilisé, par opposition à *transcodage*, afin de souligner le fait que l'opération de transcodage est effectuée sans compromettre la sécurité. Le transcodage sécurisé peut également être considéré comme l'exécution d'un transcodage dans le domaine cryptographique.

3.28 filigrane: signal imperceptiblement ajouté au signal de masquage afin d'acheminer des données masquées.

3.28.1 filigranage: processus qui insère imperceptiblement, dans des données multimédias de l'une des deux façons suivantes, des données représentant certaines informations:

- la méthode avec perte qui signifie que le signal de masquage exact ne pourra jamais être récupéré une fois le filigrane imbriqué;
- la méthode sans perte qui signifie que le signal de masquage exact pourra être récupéré après extraction du filigrane.

4 Symboles et abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent.

BAS	Segment verrouillé en octets (*byte aligned segment*)
FBAS	Segment verrouillé en octets d'un champ (*field byte aligned segment*)
G	Granularité
GL	Niveau de granularité (*granularity level*)
INSEC	Marqueur de sécurité de flux binaire entrant (*in-codestream security marker*)
IP	Propriété intellectuelle associée à une technologie (*intellectual property related to technology*)
IPR	Droits de propriété intellectuelle associés à un contenu (*intellectual property rights related to content*)
JPSEC	Codage JPEG 2000 sécurisé (*secure JPEG 2000*)
KT	Modèle de clé (*key template*)
LSB	Bit de plus faible poids (*least significant bit*)
MAC	Code d'authentification de message (*message authentication code*)
MSB	Bit de plus fort poids (*most significant bit*)
PD	Domaine de traitement (*processing domain*)
PKI	Infrastructure de clés publiques (*public key infrastructure*)
PO	Ordre de traitement (*processing order*)
RA	Organisme d'enregistrement (*registration authority*)
RBAS	Segment verrouillé en octets d'une étendue (*range byte aligned segment*)
SEC	Marqueur de sécurité (*security marker*)

T Modèle (*template*)

V Valeurs

VL Liste de valeurs (*value list*)

ZOI Zone d'influence

5 Syntaxe JPSEC (paragraphe normatif)

5.1 Aperçu général du cadre JPSEC

La syntaxe JPSEC définit un cadre pour la sécurisation de données à codage JPEG 2000. Le noyau de la présente Recommandation | Norme internationale est la spécification de la syntaxe de l'image à codage JPEG 2000 sécurisé: le *flux à codage JPSEC*. La syntaxe est orientée vers les données à codage JPEG 2000. Elle permet la protection de tout ou partie du flux codé. En toutes circonstances, les données protégées (c'est-à-dire les flux à codage JPSEC) doivent suivre la syntaxe normative définie dans la présente Recommandation | Norme internationale.

Au flux à codage JPSEC sont associés un certain nombre de *services de sécurité JPSEC*, y compris la confidentialité et l'authentification de l'origine et du contenu.

La syntaxe *de signalisation* spécifie:

- quels services de sécurité sont associés aux données d'image;
- quels *outils JPSEC* sont requis afin de fournir les services correspondants;
- comment les outils JPSEC sont appliqués;
- quelles parties des données d'image sont protégées.

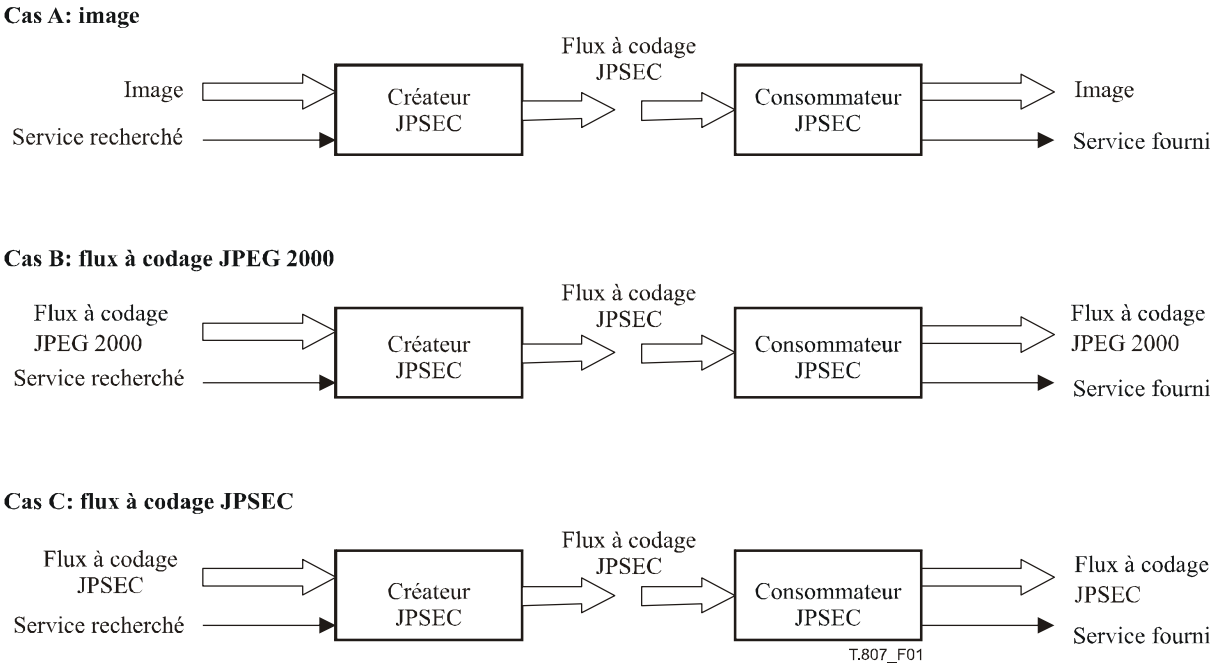


Figure 1 – Aperçu général des étapes théoriques dans le cadre JPSEC

La syntaxe du flux à codage JPSEC est normative. L'objectif consiste à permettre aux applications JPSEC de consommer des flux à codage JPSEC de façon interopérable (voir Figure 1): l'application consommatrice JPSEC interprète le flux à codage JPSEC, recherche et applique les outils JPSEC signalés, achemine les services correspondants de sécurité, puis transmet le flux ou l'image à codage JPEG 2000 pour traitement subséquent, p. ex. par un visionneur d'images.

Comme représenté dans le cas C de la Figure 1, le flux à codage JPSEC peut être créé à partir d'un autre flux à codage JPSEC. Cela peut se produire quand de multiples outils JPSEC sont appliqués au même contenu, mais à différents moments ou par différentes entités. Quand cela se produit, l'ordre dans lequel les outils JPSEC sont appliqués pendant les opérations de création et de consommation peut être significatif.

La syntaxe de signalisation identifie les outils qui sont utilisés par un consommateur JPSEC. Ces outils sont définis soit par la partie normative de la norme, ou par l'organisme d'enregistrement, ou par des outils privés. Les outils définis de façon normative prennent en charge la confidentialité (au moyen d'outils de chiffrement) ainsi que l'authentification de la source et du contenu. Ils autorisent le type le plus élevé d'interopérabilité car des implémentations indépendantes du processus de consommation sont en mesure de traiter le même flux à codage JPSEC et de rendre les services correspondants avec le même comportement.

La façon dont le flux à codage JPSEC est créé est hors du domaine d'application de la présente Recommandation | Norme internationale. Pour être conformes, les créateurs JPSEC doivent produire des flux à codage JPSEC qui comprennent la signalisation JPSEC appropriée. Des flux à codage JPSEC peuvent être créés d'un certain nombre de façons. Par exemple, un outil JPSEC peut être appliqué à des éléments d'image (pixels) ou à des coefficients d'ondelette, ou à des coefficients quantifiés, ou à des paquets.

Un consommateur peut implémenter un ou plusieurs outils JPSEC. Par exemple, il pourra exécuter un déchiffrement en utilisant l'analyse par blocs AES en mode ECB et une vérification de signature en utilisant le hachage SHA-128 et une clé publique RSA. Avec ces capacités, il sera capable d'exécuter des services de sécurité comme la confidentialité et l'authentification.

Dans le cadre de la syntaxe JPSEC, les outils JPSEC sont spécifiés par des modèles définis secrètement, ou sont enregistrés par un *organisme d'enregistrement JPSEC*. Les outils JPSEC spécifiés par les modèles ont un comportement de traitement unique et ne nécessitent donc pas d'identification unique. Ceux qui sont spécifiés par l'organisme d'enregistrement sont associés à un numéro unique d'identification fourni par le registre commun.

5.2 Services de sécurité JPSEC

L'objectif du présent paragraphe consiste à énumérer et à expliquer les fonctionnalités qui sont incluses dans le domaine d'application de la présente Recommandation | Norme internationale.

Les outils JPSEC servent à peut implémenter des fonctions de sécurité. La syntaxe JPSEC est un cadre ouvert, c'est-à-dire extensible dans le temps. Actuellement, il est centré sur les aspects suivants:

– *Confidentialité via chiffrement, sélectif ou non sélectif*

  Un fichier JPSEC peut prendre en charge une transformation de données non codées (image et/ou métadonnées) en une forme (cryptogramme) qui masque la signification originale de ces données. Par *chiffrement sélectif*, l'on entend que ce n'est pas la totalité, mais seulement des parties de l'image et/ou des métadonnées qui peuvent être chiffrées.

– *Vérification d'intégrité*

  Un fichier JPSEC peut prendre en charge des moyens permettant de détecter des manipulations apportées à l'image et/ou aux métadonnées et ainsi vérifier leur intégrité. Il y a deux classes de vérification de l'intégrité:

  1) vérification de l'intégrité des données d'image où même un seul bit de données d'image erroné se traduit par un échec de vérification (c'est-à-dire que la vérification renvoie le message: "pas d'intégrité"). Cette vérification est par ailleurs souvent désignée par le terme de *vérification fragile (d'intégrité) d'image*;

  2) vérification de l'intégrité du contenu d'image, où même une certaine altération occasionnelle des données d'image se traduit par un succès de vérification tant que cette altération ne change pas le contenu d'image du point de vue du système visuel humain ou, en d'autres termes, tant que la perception du sens de l'image ne change pas. Cette vérification est également souvent désignée par le terme de *vérification semi-fragile (d'intégrité) d'image*.

  Cette vérification fragile ou semi-fragile de l'intégrité pourrait identifier des emplacements dans les données d'image/le contenu d'image où l'intégrité est mise en question. Solutions possibles:

  1) méthodes cryptographiques telles que codes d'authentification de message (MAC, *message authentication code*), signatures numériques, sommes de contrôle cryptographique ou adressage dispersé sur clés calculées;

  2) méthodes fondées sur un filigranage. La présente Recommandation | Norme internationale ne définit pas de modèle normatif pour la technique de filigranage, bien qu'elle prenne en charge les outils non normatifs utilisant cette technique;

  3) combinaison des deux types de méthode précédents.

– *Authentification de l'origine*

Un fichier JPSEC peut prendre en charge une vérification de l'identité d'un utilisateur/correspondant qui a produit le fichier JPSEC. Cette vérification peut faire appel à des méthodes telles que les signatures numériques ou le code d'authentification de message (MAC).

– *Accès conditionnel*

Un fichier JPSEC peut prendre en charge un mécanisme et une politique permettant d'octroyer ou d'interdire l'accès à des données d'image ou à des portions de celles-ci. Ce procédé pourrait par exemple autoriser une (pré)visualisation à basse résolution d'une image sans qu'il soit possible de visualiser une résolution supérieure.

– *Identification d'un contenu enregistré*

Un fichier JPSEC peut être enregistré auprès d'un organisme d'enregistrement de contenu. Il peut prendre en charge une méthode de vérification de concordance entre les données d'image/le contenu d'image (que l'on revendique) et les données d'image/le contenu d'image que l'on a enregistré. Par exemple, de telles méthodes pourraient être les suivantes: lecture d'un identificateur de fichier (plaque d'immatriculation) qui a été placé à l'intérieur des métadonnées, vérification de la cohérence entre cette plaque d'immatriculation et les informations qui ont été téléchargées en exportation quand le processus d'enregistrement a été effectué. La plaque d'immatriculation pourrait contenir assez d'informations pour être en mesure de demander des renseignements auprès de l'organisme d'enregistrement de contenu où le fichier a été enregistré et de vérifier que ce fichier correspondent à l'identificateur.

– *Flux direct à échelonnement et transcodage sécurisés*

Un fichier JPSEC ou une séquence de paquets JPSEC peut prendre en charge des méthodes telles que le même nœud (ou un nœud différent) puisse exécuter la transmission en flux direct et le transcodage sans nécessiter de déchiffrement ni de déprotection du contenu. Un exemple est le cas où un contenu JPEG 2000 protégé est transmis en flux direct à un nœud ou à un serveur intermédiaire à mi-réseau, qui à son tour transcode le contenu JPEG 2000 protégé d'une façon qui préserve la sécurité de bout en bout.

5.3 Commentaires sur la conception et l'implémentation de systèmes JPSEC (sécurisés)

La présente Recommandation | Norme internationale prend en charge un riche et flexible ensemble de services de sécurité. Par exemple, les primitives de chiffrement peuvent être appliquées de différentes façons afin d'atteindre différents objectifs, allant du chiffrement de la totalité du flux à codage JPEG 2000 au chiffrement sélectif d'une petite portion seulement du flux codé. Il importe toutefois de souligner que des précautions particulières doivent être prises lors de l'implémentation d'un quelconque système de sécurité, même fondé sur la syntaxe JPSEC.

Il est fortement recommandé que les concepteurs de tous les systèmes de sécurité examinent de près les directives recommandées au sujet des primitives de sécurité qui peuvent être employées. Pour la plupart des primitives de sécurité signalées au moyen de la syntaxe JPSEC, les normes ISO/CEI associées offrent d'importantes indications sur leur usage correct. Par exemple, pour un chiffrement utilisant un algorithme par blocs et un mode associé de chiffrement par blocs (Tableau 29), des directives sur le choix et le fonctionnement du mode de chiffrement par blocs sont données dans l'ISO/CEI 10116.

Par ailleurs, dans de nombreuses applications de sécurité, l'authentification est le plus important service de sécurité. Même quand la confidentialité est le service de sécurité recherché, celui-ci devrait être augmenté par une authentification afin d'empêcher diverses formes d'attaques. Spécifiquement, même dans de nombreuses applications d'imagerie où l'objectif premier est la confidentialité, il est recommandé que l'authentification soit également employée.

La gestion des clés est hors du domaine d'application de la syntaxe JPSEC; cependant sa criticité doit encore être soulignée. Dans tout système cryptographique, la gestion des clés cryptographiques qui commandent les opérations est d'une importance cruciale. Si ces clés sont compromises, alors la sécurité de l'ensemble du système est compromise au point que cette compromission puisse ne pas être détectée. Il est donc impératif que les clés soient produites, distribuées, mémorisées et détruites à un niveau de sécurité qui soit au moins égal à celui des données qu'elles sont censées protéger. Par ailleurs, comme la probabilité qu'une clé soit compromise augmente avec le temps, il est également impératif que les clés ne soient utilisées que pendant une durée fixe de leur vie. Pour plus d'informations sur l'utilisation et la gestion des clés cryptographiques, voir l'ISO/CEI 11770.

Comme avec tous les systèmes de sécurité, l'utilisation d'opérations cryptographiques doit être complètement opaque à l'utilisateur. C'est-à-dire que celui-ci ne devrait pas être en mesure de découvrir de quelconques informations sur les opérations cryptographiques, sauf pour la sortie. Par exemple, l'utilisateur ne devrait pas être en mesure d'accéder à des informations concernant la raison pour laquelle une opération cryptographique n'a pas réussi à produire une sortie. De même, un utilisateur ne devrait pas être en mesure de trouver de quelconques informations complémentaires même s'il recourt au mesurage des "canaux latéraux" comme l'analyse du rythme et/ou de la puissance. En bref, l'utilisateur ne devrait pas être en mesure de remarquer une quelconque différence dans l'une quelconque des sorties applicatives,

quelle que soit l'application qu'il est actuellement en train d'exécuter car, si tel n'est pas le cas, la fuite d'informations résultante pourra éventuellement compromettre la sécurité du système.

En résumé, il est fortement recommandé que le concepteur d'un système de sécurité, fondé ou non sur la syntaxe JPSEC, prête une attention particulière aux détails de conception de ce système afin de garantir sa sécurisation.

5.4 Segment verrouillé en octets (BAS)

5.4.1 Segment verrouillé en octets

Afin d'offrir une signalisation extensible des classes et des modes, la présente Recommandation | Norme internationale utilise une structure de données à longueur variable, appelée *segment verrouillé en octets* (BAS, *byte aligned segment*). Les champs paramétriques dont le nombre est extensible sont représentés avec la structure de segment verrouillé en octets de champ (FBAS, *field byte aligned segment*). Les valeurs paramétriques ayant une grande étendue sont représentées sous forme extensible, au moyen de la structure de segment verrouillé en octets d'étendue (RBAS, *range byte aligned segment*).

Comme décrit dans la Figure 2, le segment BAS se compose d'une séquence d'un ou de plusieurs octets de segments BAS. Le bit de plus fort poids (MSB, *most significant bit*) de chaque octet de segment BAS indique l'existence d'un octet de segment BAS subséquent. Spécifiquement, si MSB = 1, alors un octet subséquent de segment BAS existe, alors que si MSB = 0, alors un octet subséquent de segment BAS n'existe pas et la structure à segments BAS est terminée. Les bits de plus faible poids qui restent dans chaque octet de segment BAS sont concaténés de façon à former une liste de bits qui sont utilisés de différentes façons pour différents paramètres à segments BAS: ils sont souvent utilisés dans le cadre d'une liste de paramètres ayant un certain nombre d'éléments et chaque bit de segment BAS est réglé à 1 ou 0 afin de signaler par un fanion des informations sur son élément correspondant. Cette structure flexible a été choisie en raison de son extensibilité en vue de futures évolutions de la norme, car elle permet de signaler de nouveaux paramètres de façon extensible.

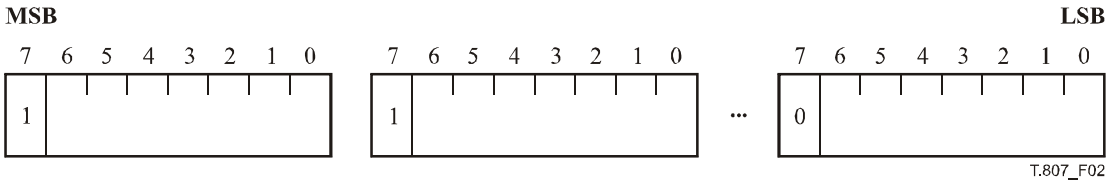


Figure 2 – Structure d'un segment verrouillé en octets (BAS)

5.4.2 Segment BAS de champ (FBAS)

Un segment BAS de champ (FBAS) est un type de segment BAS où les bits restants des octets de segments BAS servent à mettre les champs à 1 ou à 0. Un exemple d'utilisation de segment FBAS est la classe de description de la zone d'influence (DCzoi), où l'on peut spécifier de multiples descriptions d'image telles que l'indice de pavé, le niveau de résolution et la composante chromatique. Si l'on fait ainsi, l'on signalera, en mettant le fanion à 1, les trois bits de segment BAS correspondant à: pavé, résolution et couleur.

Par exemple, si l'on souhaite représenter un segment BAS de champ avec 9 champs, de f1 à f9, alors l'on aura besoin d'utiliser au plus deux octets de segments BAS. Si les deux octets ont été "a" et "b" et si le bit de plus fort poids de chaque octet a été a0 et b0, alors le segment FBAS aura l'allure suivante:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

a0 et b0 sont les bits indicateurs. Les champs f1 à f7 sont représentés par les bits a1 à a7, le champ f8 est représenté par le bit b1 et le champ f9 est représenté par le bit b2. Les bits b3 à b7 restants sont réservés et réglés à 0.

a0 f1 f2 f3 f4 f5 f6 f7 | b0 f8 f9 0 0 0 0 0

Quand il est utilisé dans un flux JPSEC, le segment FBAS figurant dans cet exemple peut être représenté par un ou deux octets, selon les valeurs réelles du champ. Cela s'explique par le fait que la valeur par défaut des champs est 0. Donc, si les champs f8 et f9 ne sont pas activés (c'est-à-dire si leur valeur est 0), alors le second octet du segment BAS n'est pas requis et a0 est réglé à 0. D'autre part, si le champ 8 ou le champ 9 est activé, alors deux octets sont requis. Dans ce cas, a0 est réglé à 1 et b0 est réglé à 0.

Noter que les bits du champ sont "alignés à gauche". Cela permet d'ajouter plus de champs au cours du temps, d'une façon compatible.

5.4.3 Segment BAS d'étendue (RBAS)

Le segment BAS d'étendue (RBAS) sert à élargir l'étendue ou le nombre de bits servant à représenter une valeur. Il y a deux types de segment RBAS: RBAS-8 et RBAS-16.

Le segment RBAS-8 contient un ou plusieurs octets de segment RBAS qui contiennent les bits de la valeur. Comme dans le segment FBAS, le premier bit de chaque octet indique si un autre octet RBAS suit.

Contrairement au segment FBAS, le segment RBAS est "aligné à droite". Donc, si une valeur a 9 bits significatifs de v1 à v9, où v1 est le bit de plus fort poids, alors cette valeur serait représentée par deux octets de segment BAS:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

comme suit:

1 0 0 0 0 0 v1 v2 | 0 v3 v4 v5 v6 v7 v8 v9

Si la valeur était assez petite pour que les bits v1 et v2 aient été zéro, alors la représentation par deux octets ci-dessus pourra être utilisée avec v1 et v2 réglés à zéro, ou un segment RBAS d'un seul octet pourra être utilisé comme représenté ci-dessous:

0 v3 v4 v5 v6 v7 v8 v9

Le segment RBAS-16 peut servir à représenter des valeurs qui comptent normalement plus de 7 mais moins de 15 bits. Dans ce cas, le premier fragment de segment RBAS aura deux octets dans lesquels: le premier bit sera l'indicateur; les 15 bits suivants seront les bits de valeur; puis les octets restants auront étendu un seul octet à la fois au moyen de la structure normale de segment BAS où le premier bit de chaque octet est l'indicateur d'octets suivants de segment BAS.

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7 | c0 c1 c2 c3 c4 c5 c6 c7

Si une valeur paramétrique avait 22 bits, alors elle pourra être représentée par la structure à trois octets de segment RBAS-16 représentée ci-dessous, où a0 et c0 sont des bits indicateurs spécifiant si un octet de segment BAS suit. Tous les octets restants de segment BAS sont des segments BAS traditionnels à un seul octet.

a0 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | c0 v16 v17 v18 v19 v20 v21 v22

Donc, les bits indicateurs seront réglés comme suit:

1 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | 0 v16 v17 v18 v19 v20 v21 v22

Pour les deux segments RBAS-8 et RBAS-16, les bits de valeur sont également "alignés à droite".

Noter que, lors de la rédaction de créateurs et de consommateurs JPSEC, il est important de veiller aux représentations gros-boutistes/petit-boutistes.

5.5 Marqueur de sécurité principal (SEC)

5.5.1 Segments marqueurs de sécurité

Dans le présent paragraphe, l'on présente une syntaxe simple et flexible, quoique puissante, pour la signalisation JPSEC. Les segments marqueurs SEC sont définis à cette fin et sont situés dans l'en-tête principal. La syntaxe de segment marqueur SEC permet de décrire toutes les informations requises pour sécuriser des images JPEG 2000. A cette fin, cette syntaxe fait référence à des outils JPSEC normatifs qui sont spécifiés par les modèles décrits dans le § 5.8 ou par des outils JPSEC non normatifs qui peuvent avoir été enregistrés au préalable auprès de l'organisme d'enregistrement JPSEC ou avoir été définis secrètement. La syntaxe énonce également des dispositions pour le traitement des paramètres associés à ces outils.

Un flux à codage JPSEC peut être protégé au moyen d'un ou de plusieurs outils JPSEC, qui sont normatifs ou non normatifs. Les paramètres de ces outils sont signalés dans un ou plusieurs segments marqueurs SEC situés dans l'en-tête principal du flux codé après le segment marqueur SIZ. Quand de multiples segments marqueurs SEC sont utilisés, ils sont concaténés et doivent apparaître consécutivement dans l'en-tête principal. Dans la plupart des cas, tous les paramètres JPSEC peuvent être signalés dans un seul segment marqueur SEC. Cependant, dans certains cas, la longueur

de la signalisation peut dépasser la longueur maximale du segment marqueur. Quand cela se produit, des segments marqueurs SEC additionnels peuvent être utilisés pour la signalisation.

La Figure 3 montre la syntaxe du segment marqueur SEC. Ce segment est signalé par le marqueur SEC 0xFF65. L_{SEC} est la longueur du segment marqueur SEC, y compris les 2 octets pour le paramètre L_{SEC}, mais non les deux octets pour le marqueur SEC proprement dit. Z_{SEC} est un indice de segment marqueur SEC qui doit être réglé à 0 pour le premier segment marqueur apparaissant dans le flux codé. P_{SEC} est un champ paramétrique qui décrit les paramètres de sécurité appartenant au flux codé entier; il n'existe que dans le premier segment marqueur SEC, c'est-à-dire si $Z_{SEC} = 0$. La syntaxe prend en charge l'utilisation de plusieurs outils JPSEC qui sont signalés dans un ou plusieurs segments marqueurs. Si plus d'un seul outil JPSEC est utilisé, alors un consommateur JPSEC doit traiter ces outils dans l'ordre où ils apparaissent dans le flux codé.

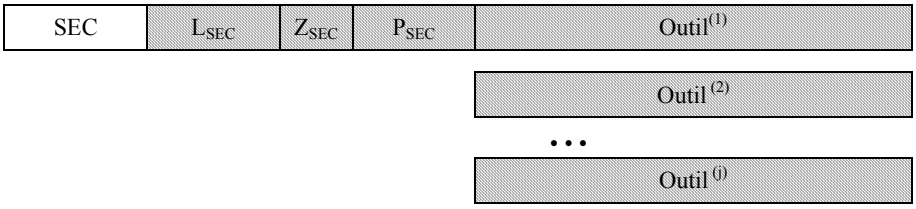


Figure 3 – Syntaxe du segment marqueur de sécurité principal

SEC: code de marqueur. Le Tableau 1 montre les longueurs et valeurs des symboles et paramètres pour le segment marqueur de sécurité principal.

L_{SEC}: longueur du segment marqueur en octets (y compris le paramètre L_{SEC} proprement dit, mais à l'exclusion du marqueur).

Z_{SEC}: indice de ce segment marqueur par rapport à tous les autres segments marqueurs SEC présents dans l'en-tête actuel. Ce champ utilise la structure de segment RBAS.

P_{SEC}: champ paramétrique pour paramètres de sécurité de flux codé. Ce champ n'est présent que dans le premier segment marqueur SEC, c'est-à-dire quand Z_{SEC} est 0.

Outil(i): paramètres pour l'outil JPSEC *i*. Si de multiples outils JPSEC sont signalés, alors un consommateur JPSEC doit traiter chaque outil dans leur ordre d'apparition dans le flux à codage JPSEC.

Tableau 1 – Principales valeurs paramétriques de sécurité

Paramètre	Longueur (bits)	Valeurs
SEC	16	0xFF65
L_{SEC}	16	2 ... $(2^{16} – 1)$
Z_{SEC}	8 + 8 * n (RBAS)	0 ... 2^{7+7*n}
P_{SEC}	0, si $Z_{SEC} > 0$ Variable, sinon	 Si $Z_{SEC} = 0$, Voir Tableau 2
Outil(i)	Variable	Voir § 5.6.2 et 5.6.3

La Figure 4 montre la syntaxe des paramètres de sécurité dans l'en-tête principal quand de multiples segments marqueurs SEC sont utilisés. Dans ce cas, les paramètres de l'outil JPSEC sont dans différents segments marqueurs SEC. Chaque segment marqueur commence par le marqueur SEC, 0xFF65, et est suivi par la longueur et l'indice du segment marqueur. L'indice du premier segment marqueur doit être réglé à 0 et doit augmenter d'une unité pour chaque segment marqueur dans l'ordre où il apparaît. Seul le premier segment marqueur contient les paramètres de sécurité pour le flux codé, P_{SEC}. Tous les segments marqueurs contiennent ces paramètres pour un ou plusieurs outils JPSEC.

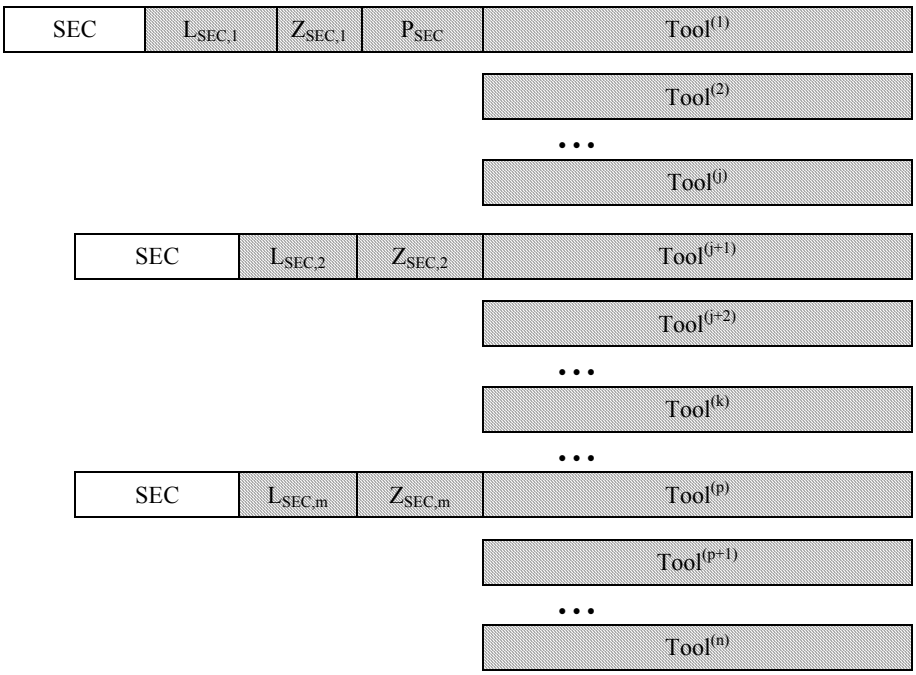


Figure 4 – Syntaxe du marqueur de sécurité principal quand de multiples segments marqueurs sont utilisés

Si requis, une description d'outil JPSEC peut englober de multiples segments marqueurs SEC, p. ex., cela peut se produire si l'outil nécessite une longueur qui dépasse la longueur maximale du marqueur SEC. Comme la longueur de la description d'outil est complètement spécifiée, le créateur JPSEC se contente de subdiviser cet outil en segments marqueurs SEC. Le décodeur devrait alors concaténer tous les segments, moins le marqueur SEC et les valeurs L_{SEC} et Z_{SEC}, puis interpréter les outils en conséquence.

P_{SEC} est un champ paramétrique qui décrit des paramètres de sécurité pour la totalité de flux codé et non pour un outil particulier. Ce champ sert à indiquer des événements tels que la conformité à la Partie 1 de la norme JPEG 2000 ou l'utilisation de marqueurs INSEC. Les paramètres P_{SEC} sont représentés dans la Figure 5.

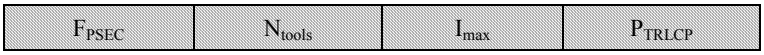


Figure 5 – Syntaxe des paramètres de sécurité de flux codé (P_{SEC})

F_{PSEC}: fanion servant à indiquer si le segment marqueur INSEC est utilisé, si de multiples segments marqueurs SEC sont utilisés, si les données originales du flux codé selon la Partie 1 de la norme JPEG 2000 ont été modifiées et si l'usage des balises indicielles TRLCP a été défini. La structure de segment FBAS est utilisée par ce champ.

N_{tools}: nombre d'outils JPSEC utilisés dans le flux codé. Ce champ utilise la structure de segment RBAS.

I_{max}: valeur maximale d'indice d'instance d'outil utilisée dans le flux codé. Ce champ utilise la structure de segment RBAS.

P_{TRLCP}: champ paramétrique servant à définir le format de balise indicielle TRLCP. Ce champ existe si $F_{TRLCP} = 1$.

Tableau 2 – Paramètres de sécurité de flux codé (P_{SEC}) dans le premier segment marqueur SEC

Paramètre	Longueur (bits)	Valeurs
F_{PSEC}	Variable (FBAS)	Voir Tableau 3
N_{tools}	8 + n * 8 (RBAS)	1 ... 2^{7+7*n}
I_{max}	8 + n * 8 (RBAS)	0 ... 2^{7+7*n}
P_{TRLCP}	0, si F_{TRLCP} = 0 32, si F_{TRLCP} = 1	Voir Tableau 4

Le paramètre F_{PSEC} est une structure de segment FBAS qui sert à indiquer un certain nombre de fanions paramétriques concernant le flux à codage JPSEC. Les champs représentés par F_{PSEC} sont présentés dans le Tableau 3. F_{INSEC} doit être réglé à 1 si des marqueurs INSEC sont utilisés dans le flux à codage JPSEC. $F_{multiSEC}$ doit être réglé à 1 si de multiples segments marqueurs SEC sont utilisés dans le flux à codage JPSEC. F_{mod} doit être réglé à 1 si les données originales JPEG 2000 ont été modifiées dans le flux à codage JPSEC. Noter que si des marqueurs INSEC sont utilisés, les données originales JPEG 2000 sont modifiées et donc F_{INSEC} et F_{mod} doivent être réglés à 1. F_{TRLCP} doit être réglé à 1 si l'usage de balise indicielle TRLCP est défini dans P_{SEC}. S'il est défini, alors le descripteur de balise indicielle TRLCP, P_{TRLCP}, est spécifié dans le champ paramétrique P_{SEC}. L'usage de balise indicielle TRLCP doit être spécifié si un quelconque outil situé dans le flux à codage JPSEC utilise des balises indicielles TRLCP.

Tableau 3 – Sémantique pour valeurs F_{PSEC} (segments FBAS)

Champ de segment BAS	Numéro de bit de segment BAS	Valeur (bits)	Sémantique
F_{INSEC}	1	0	INSEC n'est pas utilisé
		1	INSEC est utilisé
$F_{multiSEC}$	2	0	Un seul segment marqueur SEC est utilisé
		1	De multiples segments marqueurs SEC sont utilisés
F_{mod}	3	1	Des données originales JPEG 2000 ont été modifiées
		0	Sinon
F_{TRLCP}	4	0	L'usage de balise indicielle TRLCP n'est pas défini dans P_{SEC}
		1	L'usage de balise indicielle TRLCP est défini dans P_{SEC}

La syntaxe JPSEC définit une structure appelée *balise indicielle TRLCP* qui peut servir à identifier de façon unique un paquet JPEG 2000, lequel peut être spécifié de façon unique par son indice de pavé (T), par son indice de niveau de résolution (R), par son indice de couche (L), par son indice de composante (C) et par son indice de district (P). Une balise indicielle TRLCP est définie comme une unité de données avec un nombre fixe de bits servant à spécifier chacune de ces valeurs indicielles. Le nombre de bits pour chaque indice est activé dans P_{SEC}. Le descripteur P_{TRLCP} est un champ paramétrique qui décrit le format de la balise indicielle TRLCP telle qu'elle doit être utilisée dans les outils JPSEC. Ce champ n'existe que si F_{TRLCP} = 1. Le descripteur P_{TRLCP} se compose des variables suivantes, indiquées dans la Figure 6.

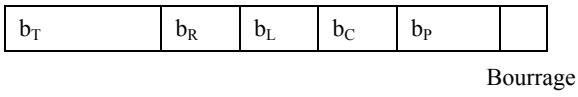


Figure 6 – Syntaxe du descripteur de balise indicielle TRLCP (P_{TRLCP})

b_T: le nombre de bits servant à représenter l'indice de pavé est bT + 1 dans la balise indicielle TRLCP.

b_R: le nombre de bits servant à représenter l'indice de niveau de résolution est bR + 1 dans la balise indicielle TRLCP.

b_L: le nombre de bits servant à représenter l'indice de couche est bL + 1 dans la balise indicielle TRLCP.

b_C: le nombre de bits servant à représenter l'indice de composante est bC + 1 dans la balise indicielle TRLCP.

b_P: le nombre de bits servant à représenter l'indice de district est bP + 1 dans la balise indicielle TRLCP.

Tableau 4 – Champs paramétriques pour le descripteur de balise indicielle TRLCP (P_{TRLCP})

Paramètre	Longueur (bits)	Valeur
b_T	8	0 ... $(2^8 – 1)$
b_R	4	0 ... 15
b_L	5	0 ... 31
b_C	5	0 ... 31
b_P	8	0 ... $(2^8 – 1)$
Padding	2	0

La longueur de chaque balise indicielle TRLCP résultante est le plus petit entier de longueur d'octet qui contient tous les bits. Le format de la balise indicielle TRLCP contient les bits pour l'indice de pavé, l'indice de niveau de résolution, l'indice de couche, l'indice de composante et l'indice de district, dans cet ordre. Si des bits supplémentaires sont requis afin de satisfaire l'exigence relative à l'entier de longueur d'octet, alors la balise indicielle TRLCP sera placée dans les bits de plus faible poids possible et les bits supplémentaires seront réglés à 0. Noter que ces bits supplémentaires seront, s'ils existent, les bits MSB de la balise indicielle TRLCP.

5.5.2 Application de multiples outils JPSEC

Dans de nombreuses applications, il est nécessaire d'appliquer de multiples outils JPSEC à un unique flux à codage JPEG 2000. Par exemple, le chiffrement et l'authentification peuvent être appliqués conjointement afin de protéger une image JPEG 2000. La situation générale de l'application de N outils JPSEC est illustrée dans la Figure 3, dans la Figure 4 et dans la Figure 7. Le consommateur JPSEC va lire ces N outils dans l'ordre de leur placement dans le segment marqueur SEC représenté dans la Figure 3 ou dans la Figure 4 et va les appliquer dans ce même ordre afin d'effectuer la consommation JPSEC du flux à codage JPSEC. Noter que, alors que le consommateur JPSEC applique les outils JPSEC dans l'ordre 1, 2, … , N, tels qu'il les lit à partir du segment marqueur SEC, ces outils JPSEC ont été appliqués dans l'ordre inverse pendant la création du flux à codage JPSEC, c'est-à-dire N, N – 1, ... 2, 1, comme illustré dans la Figure 7. Noter que la numérotation des outils dans la figure a été choisie de façon à mettre en évidence le fait que le consommateur JPSEC applique les outils JPSEC dans l'ordre inverse par rapport au créateur JPSEC. Cependant, toute numérotation des outils JPSEC est acceptable, du moment que chaque outil JPSEC d'un flux à codage JPSEC reçoit un numéro unique aux fins d'identification.

Généralement, la création des outils JPSEC s'effectue dans l'ordre inverse de leur consommation. Par exemple, si le créateur JPSEC applique N outils JPSEC, alors le consommateur JPSEC applique normalement ces mêmes N outils JPSEC mais dans l'ordre inverse. Une consommation JPSEC correcte de multiples outils JPSEC peut être garantie par une consommation séquentielle des N outils dans l'ordre correct et par l'exigence que toute étape intermédiaire au niveau du consommateur concorde avec l'état correspondant au niveau du créateur. Par exemple, dans la Figure 7, l'état au niveau du consommateur après consommation JPSEC de l'outil 1 devrait être égal à l'état après application de l'outil 2 pendant le processus de création JPSEC. Afin de donner un exemple spécifique de l'état, les étendues des octets devraient être cohérentes: tous les octets ajoutés lors de l'application de l'outil 1 devraient donc être supprimés lorsque l'outil 1 est supprimé au niveau du consommateur JPSEC.

Dans certaines applications, il peut être souhaitable, pour un consommateur JPSEC, de consommer les multiples outils JPSEC d'une façon différente de la description ci-dessus. Par exemple, le consommateur JPSEC peut décider de consommer les multiples outils dans un ordre différent, ou d'omettre certains outils dans sa consommation. Par ailleurs, le consommateur JPSEC peut préférer appliquer certains outils JPSEC mais sans les supprimer, par exemple afin de vérifier une signature numérique sans la supprimer. Un examen approfondi devrait être effectué dans ces cas afin de garantir que le traitement effectué dans le désordre ou omis ne conduit pas à des conséquences incorrectes ou imprévues. Ce comportement n'est pas recommandé, à moins que l'application JPSEC ne soit entièrement informée des ramifications potentielles.

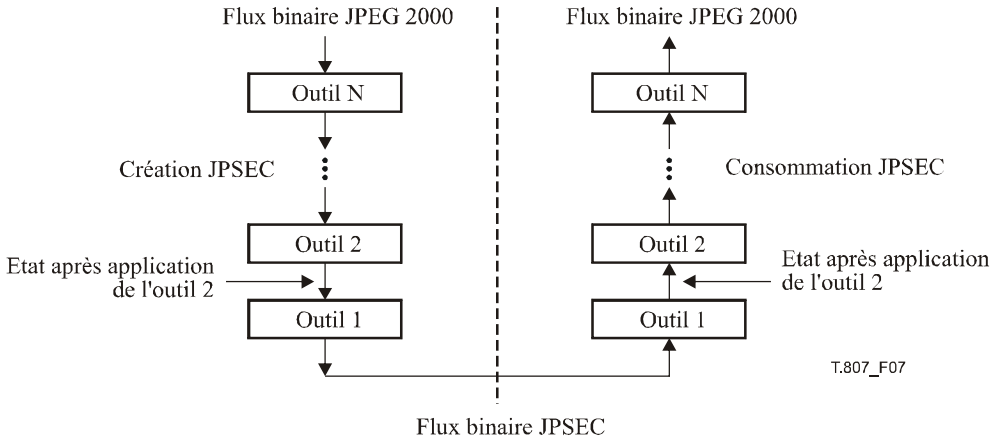


Figure 7 – Utilisation de multiples outils JPSEC

5.6 Outils JPSEC

5.6.1 Syntaxe d'outil JPSEC

Comme indiqué plus haut, il y a deux types d'outils JPSEC. Les outils JPSEC normatifs sont spécifiés avec les modèles de méthode de protection décrits dans le § 5.8 et sont également désignés par le terme d'outils JPSEC normatifs. Les outils JPSEC non normatifs sont spécifiés par un organisme d'enregistrement JPSEC ou par une application JPSEC particulière, fondée sur leur numéro d'identification: selon le cas, ils sont désignés par le terme d'outils JPSEC définis par l'organisme d'enregistrement ou d'outils JPSEC définis par l'utilisateur. La syntaxe pour les outils JPSEC normatifs est analysée dans le § 5.6.2. La syntaxe pour les outils JPSEC non normatifs est analysée dans le § 5.6.3.

La syntaxe pour les outils JPSEC est représentée dans la Figure 8. La syntaxe d'outil JPSEC a trois principales parties qui décrivent:

1) la nature de l'outil qui est appliqué avec son identification;
2) l'emplacement où l'outil est appliqué avec une structure de zone d'influence;
3) la façon dont l'outil est appliqué avec un champ paramétrique plus détaillé.

Par exemple, au moyen de la présente syntaxe, une syntaxe d'outil JPSEC pourra spécifier qu'un outil (lequel) de déchiffrement devrait être utilisé, sur la composante de résolution la plus basse dans une étendue d'octet particulière (où), au moyen d'un déchiffrement par algorithme AES en mode de chaînage CBC avec un ensemble spécifié de vecteurs d'initialisation et de clés (comment).

Figure 8 – Syntaxe d'outil JPSEC (Outil$^{(i)}$)

t: type d'outil. La valeur 0 pour le premier bit de segment BAS indique un outil JPSEC normatif. La valeur 1 pour le premier bit de segment BAS indique un outil JPSEC non normatif. Ce champ utilise la structure de segment FBAS.

i: indice d'instance d'outil (peut être utilisé comme identificateur unique). Ce champ utilise la structure de segment RBAS.

ID: valeur d'identification pour l'outil JPSEC *i*. Pour les outils JPSEC normatifs, l'identificateur ID = ID_T a 8 bits et spécifie le type de modèle. Pour les outils JPSEC non normatifs, l'identificateur ID = ID_{RA} est défini par la Figure 10 et par le Tableau 8.

L_{ZOI}: longueur de zone ZOI en octets (à l'exclusion de L_{ZOI}). Ce champ utilise la structure de segment RBAS.

ZOI: zone d'influence pour l'outil JPSEC *i*.

L_{PID}: longueur de P_{ID} en octets (à l'exclusion de L_{PID}). Ce champ utilise la structure de segment RBAS.

P_{ID}: paramètres pour l'outil JPSEC *i*.

Tableau 5 – Valeurs paramétriques d'outil JPSEC

Paramètre	Longueur (bits)	Valeurs
t	8 + 8 * n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 2)$ $(2^{7+7*n} - 1)$, réservé
ID	8, si t=0 Variable, si t=1	Voir Tableau 6 Voir Figure 10 et Tableau 8
L_{ZOI}	16+8*n (RBAS)	0 ... 2^{15+7*n}
ZOI	Variable	Voir § 5.7
L_{PID}	16+8*n (RBAS)	0 ... 2^{15+7*n}
P_{ID}	Variable	Tableau 7, si t = 0. Géré par l'organisme d'enregistrement JPSEC, si t = 1.

Chaque outil JPSEC a la syntaxe suivante. Le premier octet indique si l'outil JPSEC est normatif ou non normatif et lui assigne un identificateur d'instance. Cet octet est suivi par l'identificateur d'**identificateur d'outil**, lui-même suivi par le paramètre L_{ZOI}, qui indique la longueur du champ de zone d'influence ZOI subséquent, ainsi que par la zone d'influence proprement dite, qui décrit l'emplacement du flux de données où l'outil JPSEC est appliqué. Ces informations sont suivies par le paramètre L_{PID}, qui indique la longueur du champ paramétrique P_{ID} suivant, lequel est un champ servant à transmettre un ou plusieurs paramètres pour l'outil JPSEC.

Le premier octet de l'outil utilise une structure de segment FBAS d'un seul octet, dont le premier bit de segment BAS représente le type d'outil, t, où 0 spécifie un outil JPSEC normatif et où 1 spécifie un outil JPSEC non normatif. Cet octet est suivi par l'indice d'instance, i, qui est représenté au moyen de la structure de segment RBAS. L'indice d'instance doit être un identificateur unique de l'outil dans le flux codé et ne doit donc pas être répété par un quelconque autre outil dans le flux codé, même s'il est contenu dans un segment différent de marqueur SEC. L'indice d'instance est particulièrement critique (et nécessaire) quand des marqueurs INSEC sont utilisés, parce que chaque segment marqueur INSEC contient l'indice d'instance de l'outil auquel il s'applique. Il est recommandé que le premier outil appliqué à un créateur JPSEC ait un indice d'instance de 1 et que chaque outil additionnel soit indexé séquentiellement au fur et à mesure de son application dans le système protecteur.

Par ailleurs, chaque outil JPSEC possède un numéro d'identification qui est de 8 bits pour les outils JPSEC normatifs et de 32 bits pour les outils JPSEC non normatifs. Pour les outils JPSEC normatifs, le numéro d'identification décrit quel modèle de méthode de protection est utilisé, c'est-à-dire qu'il spécifie le modèle de déchiffrement, le modèle d'authentification, ou le modèle de hachage. Pour les outils JPSEC non normatifs, le premier bit indique s'il s'agit d'un outil JPSEC défini par l'organisme d'enregistrement ou d'un outil JPSEC défini par l'utilisateur. Dans un cas comme dans l'autre, le numéro d'identification indique l'outil particulier. Un organisme d'enregistrement JPSEC peut assurer que les numéros d'identification valides sont uniques. Cependant, une application JPSEC qui utilise des numéros d'identification définis par l'utilisateur court le risque de choisir un numéro d'identification qui est également utilisé par une autre application JPSEC, de sorte que ce numéro devrait être utilisé avec précaution.

Quand chaque outil JPSEC est appliqué au créateur JPSEC, le champ paramétrique P_{SEC} représenté dans le Tableau 2 doit être mis à jour. Par exemple, le champ paramétrique P_{SEC} contient le paramètre I_{max} qui spécifie l'indice maximal d'instance utilisé pour les outils dans le flux à codage JPSEC. Quand un nouvel outil est appliqué, celui-ci doit recevoir un indice d'instance unique. Un protecteur JPSEC peut renvoyer au paramètre I_{max} donné dans le champ paramétrique P_{SEC} afin de déterminer l'indice d'instance à attribuer à un outil JPSEC. Par exemple, il peut choisir une valeur supérieure d'une unité à la valeur I_{max} actuelle. En conséquence, le protecteur devrait ensuite incrémenter d'une unité la valeur de I_{max}.

5.6.2 Outil JPSEC normatif

L'outil JPSEC normatif utilise la syntaxe d'outil JPSEC décrite dans le § 5.6.1 et représentée dans la Figure 8, où le type d'outil t = 0 et où la longueur du numéro d'identification est de 8 bits. Les outils JPSEC normatifs sont fondés sur les modèles de méthode de protection décrits dans le § 5.8. Il y a trois types de modèle de méthode de protection; le type utilisé par l'outil est spécifié par l'identificateur d'identificateur d'outil=ID_T au moyen des valeurs représentées dans le Tableau 6.

Tableau 6 – Valeurs du numéro d'identification (ID_T) du modèle d'outil JPSEC normatif

Valeurs	Modèle de méthode de protection
0	Réservé
1	Modèle de déchiffrement
2	Modèle d'authentification
3	Modèle de hachage
4	Outil NEANT
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

Dans le cas d'outils JPSEC normatifs, le champ paramétrique P_{ID} a la structure représentée dans la Figure 9. Ce champ P_{ID} se compose de quatre sous-champs principaux: le modèle de méthode de protection T, son domaine de traitement PD, sa granularité G et sa liste de valeurs V. La syntaxe pour chacun de ces champs est donnée dans les § 5.8, 5.9, 5.10 et 5.11, respectivement. Ensemble, ces champs décrivent comment l'outil est appliqué. Le modèle de méthode de protection T décrit la méthode de protection particulière pour le modèle de déchiffrement, le modèle d'authentification, ou le modèle de hachage spécifié par l'outil normatif ID. Il peut également spécifier l'outil NEANT, auquel cas aucun modèle n'est utilisé mais d'autres fonctionnalités peuvent toutefois être utilisées. Par exemple, la zone d'influence peut être spécifiée afin de représenter des régions d'image et leurs étendues d'octet correspondantes. Le domaine de traitement PD est celui dans lequel la méthode de protection est appliquée. La granularité G est celle avec laquelle la méthode de protection est appliquée. La liste de valeurs V est celle qui peut être requise par chaque méthode de protection avec une granularité plus fine. Pour le modèle de déchiffrement, la liste de valeurs peut servir à spécifier un ensemble de valeurs d'initialisation à granularité augmentée qui doivent être utilisées. Pour le modèle d'authentification, la liste de valeurs contient un ensemble de valeurs de code MAC ou de signatures numériques. Pour le modèle de hachage, la liste de valeurs contient un ensemble de valeurs de hachage. En toutes circonstances, la liste de valeurs contient une granularité de valeurs spécifiée par le champ de granularité G.

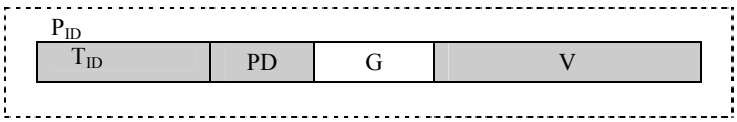


Figure 9 – Syntaxe des paramètres (P_{ID}) pour les outils JPSEC normatifs (t = 0)

T_{ID}: paramètres de modèle pour outil JPSEC normatif avec modèle identificateur ID_T.

PD: domaine de traitement pour outil JPSEC normatif.

G: granularité pour outil JPSEC normatif.

V: liste de valeurs pour outil JPSEC normatif, p. ex., vecteurs d'initialisation, valeurs de code MAC, signatures numériques, ou valeurs de hachage selon l'identificateur du modèle.

Noter que les paramètres de modèle dépendent de l'identificateur du modèle. Cependant, le domaine de traitement, la granularité et la liste de valeurs sont indépendants de l'identificateur du modèle.

Tableau 7 – Valeurs paramétriques d'outil JPSEC normatif

Paramètre	Longueur (bits)	Valeurs
T_{ID}	0, si $ID_T = 4$ Variable, sinon	N/A Voir § 5.8
PD	Variable	Voir § 5.9
G	24	Voir § 5.10
V	Variable	Voir § 5.11

5.6.3 Outil JPSEC non normatif

Dans certains cas, il peut être utile à une application JPSEC d'avoir la capacité d'appliquer un outil qui s'étend au-delà des outils JPSEC normatifs. Cette capacité est prise en charge par l'utilisation d'un outil JPSEC non normatif. Cela permet d'utiliser de nombreux éléments d'outils JPSEC normatifs, y compris la zone ZOI et les modèles JPSEC, mais ajoute la flexibilité d'une utilisation différente des paramètres en association avec une valeur d'identificateur d'outil.

L'outil JPSEC non normatif utilise la syntaxe d'outil JPSEC décrite dans le § 5.6.1 et représentée dans la Figure 8, où le type d'outil t = 1 et où l'identificateur ID_{RA} se compose d'un espace nominatif et d'un numéro d'identification, comme défini par la Figure 10 et par le Tableau 8.

Il y a deux classes d'outils JPSEC non normatifs:

1) les outils JPSEC définis par l'organisme d'enregistrement, dont la signalisation est spécifiée par un organisme d'enregistrement;
2) les outils JPSEC définis par l'utilisateur, dont la signalisation est spécifiée par une application JPSEC.

Ces deux classes d'outils JPSEC non normatifs sont signalées au moyen de l'identificateur de 32 bits $ID_{RA,\ id}$ qui est représenté dans le Tableau 9, où les identificateurs dont le premier bit est un 0 sont définis par un organisme d'enregistrement et dans lequel ceux dont le premier bit est un 1 sont définis par une application JPSEC particulière.

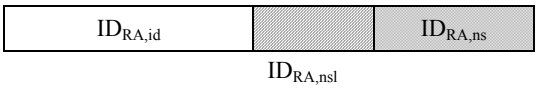


Figure 10 – Syntaxe d'identificateur ID_{RA}

$ID_{RA,id}$: identificateur d'outil défini par l'organisme d'enregistrement (RA) ou par l'utilisateur;

$ID_{RA,nsl}$: longueur du champ $ID_{RA,ns}$ en octets. Ce champ utilise la structure RBAS;

$ID_{RA,ns}$: chaîne contenant l'espace nominatif de l'outil spécifié et défini par l'organisme d'enregistrement (RA) ou par l'utilisateur.

Tableau 8 – Valeurs paramétriques contenues dans la syntaxe d'identificateur ID_{RA}

Paramètre	Longueur (bits)	Valeurs
$ID_{RA,id}$	32	Voir Tableau 9
$ID_{RA,\ nsl}$	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
$ID_{RA,ns}$	Variable	Chaîne contenant un espace nominatif

Tableau 9 – Valeurs du numéro d'identification pour les outils JPSEC non normatifs ($ID_{RA,\ id}$)

$ID_{RA,\ id}$	Signification
0x00 00 00 00 ... 0x7F FF FF FF	Outil JPSEC défini par l'organisme d'enregistrement. Ces valeurs doivent être gérées par l'organisme d'enregistrement JPSEC.
0x80 00 00 00 ... 0xEF FF FF FF	Outil JPSEC défini par l'utilisateur. Ces valeurs peuvent être définies par une application JPSEC particulière.
0xF0 00 00 00 ... 0xFF FF FF FF	Réservé pour utilisation par l'ISO.

Pour les outils définis par l'organisme d'enregistrement (RA), le champ $ID_{RA,ns}$ est l'espace nominatif de l'organisme d'enregistrement (RA) auprès duquel cet outil est enregistré. Comme chaque RA possède un unique espace nominatif, les identificateurs $ID_{RA,id}$ et $ID_{RA,ns}$ sont utilisés ensemble afin d'identifier un outil défini par organisme d'enregistrement (RA). Pour les outils définis par l'utilisateur, le champ $ID_{RA,ns}$ est choisi par les développeurs. Afin de limiter le risque de collisions entre identificateurs, il est recommandé que les développeurs recherchent la spécificité lors du choix de leur espace nominatif, p. ex., en choisissant le nom de domaine de leur organisation ou compagnie. Noter toutefois que, pour les outils définis par l'utilisateur, il n'y a aucun moyen de garantir cette spécificité de l'espace nominatif, de sorte que des collisions entre identificateurs peuvent se produire et devraient être prises en considération attentivement lors de l'utilisation d'outils définis par l'utilisateur.

Le champ P_{ID} sert à transmettre un ou plusieurs paramètres pour l'outil JPSEC non normatif *i*. Le format du champ P_{ID} n'est pas entièrement indiqué dans le domaine d'application de la syntaxe JPSEC. Si un organisme d'enregistrement est utilisé, alors le format est enregistré auprès de l'organisme d'enregistrement en même temps que l'identificateur. Si un organisme d'enregistrement n'est pas utilisé et si l'outil est défini par l'utilisateur, alors seule la longueur de ce champ est spécifiée et il appartient aux utilisateurs d'utiliser convenablement ce champ.

Cependant, la syntaxe JPSEC permet bien d'utiliser, dans le champ P_{ID} des outils JPSEC non normatifs, les structures syntaxiques définies pour les outils JPSEC normatifs. Par exemple, un outil JPSEC non normatif peut utiliser les champs de modèle de méthode de protection, de domaine de traitement, de granularité et de liste de valeurs décrits respectivement dans les § 5.8, 5.9, 5.10 et 5.11.

Cette syntaxe est très flexible et peut gérer une grande variété de techniques de sécurité comme l'intégrité des données d'image, le contrôle d'accès et les méthodes de protection des droits. Elle offre donc un riche ensemble de fonctionnalités tout en restant simple et concise.

5.7 Syntaxe de zone d'influence (ZOI)

5.7.1 Introduction

La zone d'influence (ZOI) peut servir à décrire l'aire d'application d'un outil JPSEC. Les données contenues dans l'aire d'application (spécifiée par la zone ZOI) sont désignées par le terme de données influencées. Les outils JPSEC normatifs doivent utiliser la zone ZOI afin de décrire leur aire d'application. Les outils JPSEC non normatifs peuvent utiliser la zone ZOI afin de décrire leur aire d'application ou peuvent utiliser une autre méthode. Si une autre méthode est utilisée, alors la longueur de zone ZOI est 0, c'est-à-dire n'existe pas.

La zone d'influence (ZOI) décrit l'aire d'application de chaque outil JPSEC. Celle-ci peut être décrite par des paramètres associés à l'image, p. ex., par résolution ou par région d'image; ou par des paramètres non associés à l'image, p. ex., par des segments de flux codé ou par des indices de paquet. Si des paramètres associés à l'image et des paramètres non associés à l'image sont utilisés ensemble, la zone ZOI décrit la correspondance entre ces régions. Par exemple, la zone ZOI peut servir à indiquer que les résolutions et la région d'image spécifiées par les paramètres associés à l'image correspondent aux segments de flux codé spécifiés par les paramètres non associés à l'image. Cela permet d'utiliser la zone ZOI comme métadonnée afin de signaler l'endroit du flux à codage JPSEC où certaines parties de l'image sont situées.

La Figure 11 décrit la structure théorique de la zone ZOI. Celle-ci contient une ou plusieurs sous-zones. Quand de multiples sous-zones sont utilisées à l'intérieur d'une même zone ZOI, celle-ci est définie par leur réunion. Cela indique que l'outil JPSEC devrait être appliqué à toutes ces zones. Chaque sous-zone d'une zone ZOI est décrite par trois unités fondamentales: la classe de description, le mode paramétrique et les items paramétriques (valeurs). La présente Recommandation | Norme internationale définit deux classes de description: associée à l'image et non associée à l'image. Ces paramètres peuvent être spécifiés au moyen d'un certain nombre de modes, p. ex., par une valeur unique, par de multiples valeurs énumérées, ou par une étendue. Les valeurs paramétriques ou items sont alors énumérés conformément au mode.

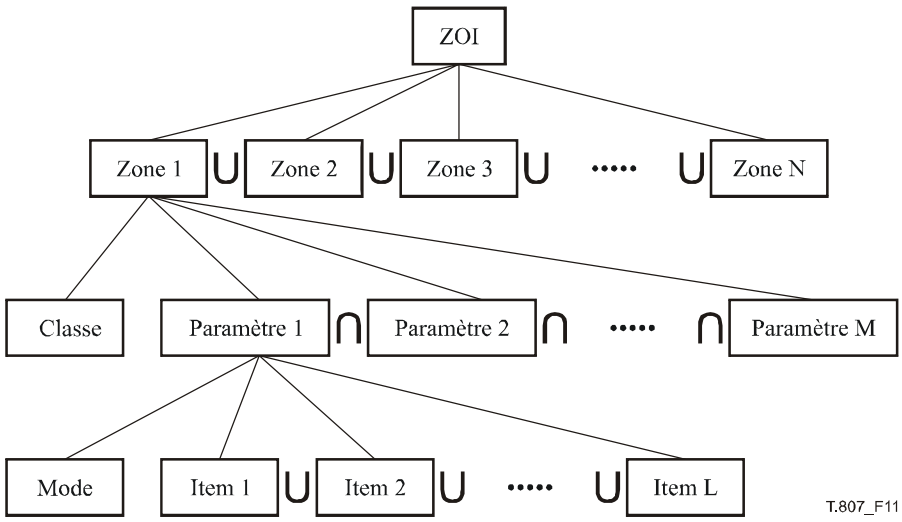


Figure 11 – Structure théorique d'une zone d'influence

5.7.2 Syntaxe de zone ZOI

La Figure 12 montre la syntaxe de zone ZOI. Celle-ci peut contenir une ou plusieurs sous-zones. Elle peut également être vide, auquel cas le champ NZzoi doit être 0. Quand cela se produit, l'influence de l'outil est spécifiée par d'autres moyens, comme par le marqueur INSEC ou par des paramètres définis par un outil JPSEC de protection non normatif.

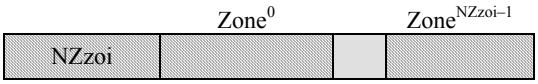


Figure 12 – Syntaxe de zone ZOI

NZzoi: nombre de zones. Ce champ utilise la structure de segment RBAS.

Zone^{k}: zone. Sa structure est spécifiée dans le § 5.7.3.

Tableau 10 – Valeurs paramétriques du champ de zone d'influence (ZOI)

Paramètre	Longueur (bits)	Valeurs
NZzoi	8 + 8 * n (RBAS)	$0 \ldots (2^{7+7*n} - 2)$ $(2^{7+7*n} - 2)$, réservé
Zone^{k}	Variable	Voir le § 5.7.3

5.7.3 Syntaxe de zone

La zone contient un indicateur de champ de la classe de description de zone, suivi par des paramètres de cette classe. La classe de description de zone utilise la structure de segment FBAS. Comme représenté dans la Figure 13, le second bit de plus fort poids dans chaque octet, étiqueté "x", signale par fanion l'utilisation d'une classe de description spécifique. La présente Recommandation | Norme internationale définit deux classes de description: associée à l'image et non associée à l'image (voir Tableau 12). Le Tableau 13 et le Tableau 14 définissent les numéros d'indicateur de champ pour, respectivement, la classe de description associée à l'image et la classe de description non associée à l'image. En concaténant les six bits contenus dans chaque octet étiqueté "y" qui suit le fanion de classe de description, on indique l'utilisation d'une description spécifique à l'intérieur d'une classe de description donnée. Une valeur de bit égale à "1" à une position binaire donnée dans chaque classe indique que le champ paramétrique correspondant existe. Le nombre de paramètres doit être le même que celui des indicateurs de champ de classe de description de zone qui ont été réglés à '1' et ce nombre doit apparaître dans l'ordre de signalisation de l'indicateur de champ de classe. La classe de description de zone possède un nombre variable d'octets. Quand le bit MSB est égal à 1, alors un autre octet de classe de description de zone suit. Le bit MSB du dernier octet de classe de description est égal à 0. Si les deux classes de description (associée à l'image et non associée à l'image) sont utilisées, alors les octets de classe de description associée à l'image doivent précéder l'octet de classe de description non associée à l'image. Quand un certain nombre d'items sont représentés au moyen de cette structure, le premier item de la liste doit correspondre au plus lourd bit disponible du premier octet.

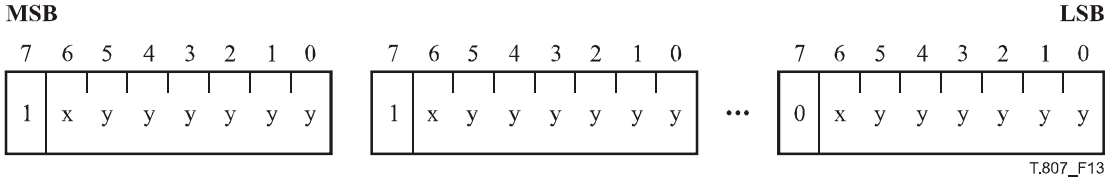


Figure 13 – Structure de classe de description de zone (DCzoi)

La Figure 14 montre la syntaxe de zone.

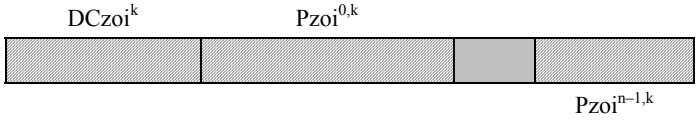


Figure 14 – Syntaxe de zone composée d'une classe de description et d'un ou de plusieurs ensembles paramétriques

DCzoi^{k}: k^{e} classe de description de zone. Ce champ utilise la structure de segment FBAS.

Pzoi^{i,k}: Les paramètres de zone conformément à la classe de description de zone spécifiée (DCzoi^{k}). Voir le § 5.7.6.

Le champ DCzoi^{k} spécifie le nombre *n* de champs de classe de description de zone qui existent, d'après le nombre de bits qui sont réglés à 1. Pour chaque champ de classe de description de zone, il existe un seul champ paramétrique de zone Pzoi^{i,k}. Ces champs apparaissent séquentiellement, dans le même ordre que les fanions dans le champ DCzoi^{k}.

Tableau 11 – Valeurs paramétriques de zone

Paramètre	Longueur (bits)	Valeurs
$DCzoi^{k}$	Variable (FBAS)	Varie conformément à l'ensemble de valeurs contenu dans le Tableau 12.
$Pzoi^{i,k}$	Variable	Voir le § 5.7.6 pour la syntaxe de ce champ

Tableau 12 – Valeur de l'indicateur de classe de description

Valeur	Classe de description
0	Classe de description associée à l'image. Les positions binaires suivantes sont définies dans le Tableau 13.
1	Classe de description non associée à l'image. Les positions binaires suivantes sont définies dans le Tableau 14.

Tableau 13 – Classe de description associée à l'image

Position binaire	Sémantique
1	Région d'image
2	Pavé(s) comme défini dans la Partie 1 de la norme JPEG 2000
3	Niveau(x) de résolution comme défini dans la Partie 1 de la norme JPEG 2000
4	Couche(s) comme défini dans la Partie 1 de la norme JPEG 2000
5	Composante(s) comme défini dans la Partie 1 de la norme JPEG 2000
6	District(s) comme défini dans la Partie 1 de la norme JPEG 2000
7	Balise(s) TRLCP (Pavé-Résolution-Couche-Composante-District)
8	Paquet(s) comme défini dans la Partie 1 de la norme JPEG 2000
9	Sous-bande(s) comme défini dans la Partie 1 de la norme JPEG 2000
10	Bloc(s) de code comme défini dans la Partie 1 de la norme JPEG 2000
11	Région(s) ROI
12	Débit binaire
13	Défini par l'utilisateur. Les détails doivent être spécifiés par d'autres moyens. (p. ex. identificateur JPSEC)
	Toutes les autres valeurs sont réservées.

Tableau 14 – Classe de description non associée à l'image

Position binaire	Sémantique
1	Paquet(s) comme défini dans la Partie 1 de la norme JPEG 2000
2	Etendue(s) d'octet (justifiée(s) par bourrage) (à partir du premier octet après le premier marqueur SOD (début de données))
3	Etendue(s) d'octet (justifiée(s) par bourrage) (à partir du premier octet après le premier marqueur SEC)
4	Etendue(s) d'octet non justifiée(s) par bourrage quand celui-ci est utilisé
5	Balise(s) TRLCP (Pavé-Résolution-Couche-Composante-District)
6	Valeur(s) de distorsion
7	Importance(s) relative(s)
8	Défini par l'utilisateur. Les détails doivent être spécifiés par d'autres moyens. (p. ex. identificateur JPSEC)
	Toutes les autres valeurs sont réservées.

Les indices de paquet sont numérotés séquentiellement dans un pavé et peuvent donc ne pas être uniques d'un pavé à l'autre. Par ailleurs, les indices de paquet d'un pavé peuvent revenir à zéro quand leur valeur maximale de 65535 est dépassée. C'est pourquoi l'indexation des paquets est décrite plus en détail. Quand les indices de paquet d'un pavé ne dépassent pas 65535 paquets, alors l'indice de paquet décrit dans le Tableau 13 est défini par l'indice de paquet donné par le champ Nsop du paramètre SOP défini dans le Tableau A.40 de la Partie 1 de la norme JPEG 2000. Noter que, lorsque la valeur maximale ne dépasse pas 65536, un unique paquet JPEG 2000 peut être spécifié de façon unique avec un indice de pavé et un indice de paquet. Quand les indices de paquet dépassent 65535 paquets, alors l'indice de paquet selon la Partie 1 de la norme JPEG 2000 est défini de façon à revenir à zéro. Dans ce cas, l'indice de paquet n'identifie pas de façon unique un paquet et ne doit pas être utilisé: il est alors recommandé d'utiliser plutôt la balise indicielle

TRLCP. Noter que les services de sécurité qui nécessitent des indices de paquet uniques sont vulnérables si l'indice de paquet revient à zéro et se répète.

Quand la balise indicielle TRLCP est utilisée, son format doit être défini dans le champ paramétrique P_{SEC} représenté dans le Tableau 2. Spécifiquement, le format de la balise indicielle TRLCP est spécifié par le champ paramétrique P_{TRLCP} du Tableau 4, qui définit la longueur des balises indicielles TRLCP dans la zone ZOI.

La classe de description non associée à l'image peut également avoir de multiples champs activés simultanément. Quand cela se produit, les modes pour les divers champs paramétriques doivent avoir le même nombre d'items (une seule exception à cette règle est décrite ci-dessous) et ces items doivent être en correspondance biunivoque les uns avec les autres, dans le même ordre. Par exemple, si la zone utilise des étendues d'octet et des étendues de paquet, chaque étendue devrait avoir le même nombre d'items, la première étendue d'octet correspondant à la première étendue de paquet et ainsi de suite.

Il y a une exception à la règle ci-dessus d'exigence du même nombre d'items dans chaque champ. Cela se produit quand un des champs f1 contient 1 item qui spécifie une étendue d'items (comme décrit par l'étendue de mode dans le § 5.7.6) et que cette étendue contient N éléments et qu'un autre champ f2 est spécifié par une liste de N items. Dans ce cas, le champ f1, qui contient seulement 1 item (l'étendue) est interprété comme étant une liste de N items. Ces N items spécifiés par l'étendue contenue dans le champ f1 doivent correspondre de façon biunivoque aux N items énumérés dans le champ f2. Donc, une étendue d'items peut être associée soit à un unique item ou à multiples items (une étendue pour chaque item qu'elle contient).

Les octets sont indexés soit à partir du premier octet après le premier marqueur SOD (début de données) ou à partir du premier octet après le premier marqueur SEC (sécurité). Dans un cas comme dans l'autre, ce premier octet est étiqueté comme octet 0.

Les champs de distorsion (ainsi que d'importance relative) offrent la capacité de signaler l'importance de régions spécifiées par la zone ZOI. Le paramètre de distorsion spécifie la contribution à la réduction de distorsion du segment de données spécifié, que ce soit pour un ensemble de paquets ou pour une étendue d'octet ou pour la région associée à l'image spécifiée. La distorsion est exprimée par le carré de l'erreur totale, au moyen d'une description d'un ou de deux octets, signalée dans le champ Mzoi. Le paramètre de distorsion relative peut servir à spécifier l'importance relative de segments de données spécifiés, en utilisant des valeurs de 1, 2 ou 4 octets signalées dans le champ Mzoi. Les détails supplémentaires et les formats de ces champs sont décrits dans le § 5.7.3.2.

La balise indicielle TRLCP spécifie le pavé, la résolution, la couche, la composante et le district d'un paquet protégé dans le flux codé. Cette balise est utilisée dans la zone ZOI afin de spécifier ces paramètres parce que ces informations peuvent être difficiles à déduire d'un flux codé protégé.

Noter que, si seules des descriptions associées à l'image sont utilisées, on peut fermer le champ. On n'a donc pas besoin de représenter des descriptions non associées à l'image si celles-ci ne sont pas utilisées.

5.7.3.1 Champs d'étendue d'octet

La classe de description non associée à l'image permet de décrire la zone ZOI sous forme d'étendues d'octet. En général, les 2^e et 3^e éléments du Tableau 14 devraient servir à représenter les étendues d'octet pour la plupart des outils, tels que l'authentification et le chiffrement/déchiffrement sans bourrage. Cependant, certaines méthodes de protection, comme le chiffrement/déchiffrement avec bourrage, modifient la longueur des données. Quand cela se produit, il est nécessaire de spécifier à la fois l'étendue d'octet justifiée par bourrage et l'étendue d'octet non justifiée par bourrage ou originale. Dans ce cas, l'étendue d'octet justifiée par bourrage est spécifiée par le 2^e ou 3^e élément du Tableau 14 conformément aux besoins de l'outil de protection. (Noter que ces deux éléments peuvent ne pas être utilisés ensemble.) En outre, l'étendue d'octet non justifiée par bourrage est spécifiée par le 4^e élément du Tableau 14. L'étendue d'octet non justifiée par bourrage devrait être spécifiée par le même mode de description que l'étendue d'octet justifiée par bourrage et avoir le même nombre d'items. Ceux-ci devraient correspondre l'un avec l'autre de façon biunivoque, dans le même ordre.

5.7.3.2 Champ de distorsion et champ d'importance relative

Les champs de distorsion et d'importance relative offrent la capacité de signaler l'importance de régions spécifiées par la zone ZOI.

Le champ de distorsion sert à associer une distorsion à une région spécifiée par la zone ZOI. La valeur de distorsion spécifie la distorsion par erreur quadratique totale (ou somme des erreurs quadratiques) qui résulterait si la région associée n'était pas disponible pour décodage. La distorsion par erreur quadratique totale est une mesure de distorsion de base qui est utilisée en traitement des images fixes et animées. Elle sert à calculer la distorsion commune en termes de variance (MSE, *mean-squared-error*) et de crête du rapport signal sur bruit (PSNR, *peak-signal-to-noise*). Le champ de distorsion est exprimé au moyen de descriptions d'un ou de deux octets, qui sont décrites ci-dessous. Le choix d'une description sur un ou deux octets est signalé par la valeur paramétrique du champ Mzoi, qui spécifie la longueur de ce champ. Le champ d'importance relative peut servir à décrire l'importance relative de différentes régions spécifiées par

zones ZOI associées, sans nécessairement être liées à une mesure de distorsion spécifique. La longueur du champ d'importance relative est également signalée par le champ Mzoi. Ces champs sont analysés plus en détail ci-dessous.

5.7.3.2.1 Champ de distorsion sur un octet

La distorsion par erreur quadratique totale est exprimée au moyen d'un champ de distorsion sur un octet en représentation de type virgule pseudo-flottante. Les 8 bits disponibles dans le champ de distorsion sont attribués comme représenté dans la Figure 15 et dans le Tableau 15 afin d'offrir un compromis approprié entre précision et dynamique. Noter qu'un bit de signe est inutile car la distorsion ne peut pas être négative. Afin de couvrir une dynamique suffisante, la base 16 est utilisée et 4 éléments binaires sont utilisés pour l'exposant (exp). La mantisse (m) est exprimée au moyen de 4 éléments binaires. Donc, la valeur totale de distorsion D est donnée par:

$$D = m \times 16^{exp}$$

où m possède une valeur dans l'étendue $0 \le m \le 15$ et où exp possède une valeur dans l'étendue $0 \le exp \le 15$. Une valeur de distorsion de zéro est représentée par m = 0 et exp = 0, c'est-à-dire par le champ de distorsion mis à zéro. En attribuant 4 bits pour la mantisse m, la précision est égale à $½ \times (1/2^4) = 1/32$ soit environ 3 %. Avec 4 bits pour l'exposant et en base16, la dynamique va de 0 à max, où max est donné par m = 15 et où exp = 15, ce qui correspondent à une distorsion de $15 \times 16^{15} = 1{,}7 \times 10^{19}$.

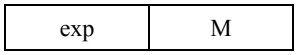


Figure 15 – Syntaxe du champ de distorsion

exp: exposant de la valeur du champ de distorsion (base 16)

m: mantisse de la valeur du champ de distorsion

Tableau 15 – Valeurs paramétriques du champ de distorsion

Paramètre	Longueur (bits)	Valeurs
exp	4	0 ... 15
m	4	0 ... 15

Noter qu'avec ce format de distorsion, on peut effectuer une comparaison entre deux distorsions afin de déterminer quelle est la plus grande en comparant simplement les deux valeurs de distorsion en tant que caractères non signés. Spécifiquement, afin d'exécuter cette comparaison, il n'est nullement nécessaire de convertir les valeurs en format de virgule pseudo-flottante en valeurs de distorsion totale proprement dite, afin de déterminer laquelle des deux valeurs de distorsion est la plus grande ou la plus petite. Cette propriété peut simplifier le traitement dans diverses applications.

5.7.3.2.2 Champ de distorsion sur deux octets

Dans le format sur deux octets, les valeurs de distorsion doivent être exprimées par un nombre de deux octets en format de virgule pseudo-flottante, défini comme suit. Ce format est utilisé dans le § E.1.1.1 (équation E.3) de la Rec. UIT-T T.800 | ISO/CEI 15444-1 afin d'exprimer la longueur de l'étape de quantification pour le codage JPEG 2000. Chaque nombre de 16 bits contient l'exposant (5 bits) et la mantisse (11 bits) de la valeur métrologique. En particulier, la valeur en virgule flottante *V* de la mesure est donnée par la formule suivante:

$$V = 2^{\varepsilon-15}\left(1+\frac{\mu}{2^{11}}\right) \quad \text{if } \varepsilon \neq 0$$
$$V = 0 \quad \text{if } \varepsilon = 0$$

où ε est l'entier non signé obtenu à partir des cinq premiers bits de plus fort poids du paramètre et où μ est l'entier non signé obtenu à partir des 11 bits restants. Le cas particulier de $V = \infty$ correspond à μ = 0 et ε = 31. Noter que les valeurs qui sous-rempliraient la représentation sont réglées à zéro.

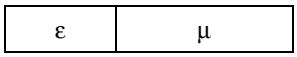


Figure 16 – Syntaxe du champ de distorsion

ε: exposant de la valeur de deux octets du champ de distorsion

μ: mantisse de la valeur de deux octets du champ de distorsion

Tableau 16 – Valeurs paramétriques du champ de distorsion

Paramètre	Longueur (bits)	Valeurs
ε	5	0 ... 31
μ	11	0 ... $(2^{11} - 1)$

L'algorithme permettant de calculer s, ε et μ n'est pas défini en tant que partie obligatoire de la présente Recommandation | Norme internationale. Une technique possible exécute les étapes suivantes (un exemple de conversion du nombre 12,25 est fourni). Si $V = 0$, poser $\varepsilon = \mu = 0$. Sinon:

- convertir V en nombre binaire ($12{,}25_{10} = 1100{,}01_2$);
- normaliser le nombre; cela signifie qu'il devrait y avoir un chiffre 1 à gauche de la virgule binaire et multiplication par la puissance de deux appropriée afin de représenter la valeur originale. La forme normalisée de 1100,01 est $1{,}10001 \times 2^3$;
- l'exposant est la puissance de 2, présentée en notation par excès. Le biais d'exposant est 15; donc, dans cet exemple, l'exposant est représenté par 18_{10} (10010_2);
- la mantisse représente les bits significatifs, *sauf pour le bit situé à gauche de la virgule binaire*, qui est toujours 1 et qui n'a donc pas besoin d'être mémorisé; des zéros sont éventuellement ajoutés afin d'obtenir 11 bits. Dans cet exemple, la mantisse est 10001000000.

5.7.3.2.3 Champ d'importance relative

Le champ d'importance relative *r* peut servir à décrire l'importance relative de différentes unités de codage, sans nécessairement être liée à une mesure de distorsion spécifique. Cela permet de décrire l'importance relative ou les priorités réciproques d'unités de codage sans décrire explicitement dans quelle proportion l'une est plus importante que l'autre. Cette importance relative des données associées est spécifiée par un champ de *n* octets qui prend en charge 2^{8n} rangs possibles, comme représenté dans la Figure 17 et dans le Tableau 17, où le nombre d'octets *n* de ce champ est spécifié par Mzoi. Par exemple, par l'utilisation d'un champ d'importance relative d'un seul octet, un total de 256 rangs possibles est pris en charge. Des valeurs croissantes correspondent à une importance croissante, de façon similaire au champ de distorsion.

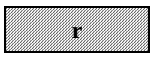


Figure 17 – Syntaxe du champ d'importance relative

r: valeur d'importance relative

Tableau 17 – Valeurs paramétriques du champ de valeur d'importance relative

Paramètre	Longueur (bits)	Valeurs
r	8 * n	0 ... $(2^{8n} - 1)$

5.7.3.2.4 Commentaires additionnels sur les champs de distorsion et d'importance relative

Etant donné qu'aussi bien pour le champ de distorsion sur un octet que pour le champ d'importance relative d'un octet, l'importance est directement proportionnelle aux valeurs, il est possible d'effectuer de la même façon des comparaisons pour ces deux unités de données, sans tenir compte du fait que le champ de distorsion spécifie une distorsion réelle ou une importance relative. Cela peut simplifier les applications.

Des en-têtes peuvent être spécifiés au moyen des champs de distorsion ou d'importance relative. La perte de divers types de données, tels que les en-têtes principaux et les en-têtes d'élément de pavé ou l'en-tête de marqueur SEC, empêche le décodage des données d'image associées. Le créateur JPSEC peut souhaiter:

1) attribuer une distorsion à ces données en utilisant la plus haute valeur de distorsion (spécifiée ci-après) afin de signaler l'en-tête ou des données critiques;
2) décrire la distorsion totale qui serait créée si l'image ou une portion de celle-ci était indécodable.

Le créateur dispose donc d'une certaine flexibilité dans la façon de signaler les en-têtes.

La plus haute valeur de distorsion pour les champs d'un seul octet est un octet en série de chiffres 1 (0xFF). Noter que cette valeur de distorsion est la plus haute possible pour à la fois le champ de distorsion totale par erreur quadratique d'un octet et le champ d'importance relative d'un octet. La plus haute valeur du champ de distorsion de deux octets est constituée par les deux octets en série de chiffres 1 (0xFFFF). La plus haute valeur du champ d'importance relative, de longueur égale à n octets, est une valeur de n octets en séries de chiffres 1.

5.7.3.2.5 Utilisation conjointe des champs de distorsion et d'importance relative

Le champ de distorsion et le champ d'importance relative peuvent être utilisés simultanément afin de décrire la région spécifiée par la zone ZOI. Dans ce cas, les deux champs spécifient la distorsion par erreur quadratique, mais le champ de distorsion spécifie la réduction marginale de distorsion alors que le champ d'importance relative spécifie la distorsion totale. Spécifiquement, le champ de distorsion spécifie la réduction marginale de la distorsion que la zone ZOI produirait si elle était décodée. Cela suppose que toutes les informations requises afin de décoder la zone ZOI soient disponibles et centrées sur la réduction marginale de la distorsion produite par la zone ZOI. Le champ d'importance relative spécifie la distorsion totale qui serait subie si la zone ZOI n'était pas disponible, c'est-à-dire qu'il spécifie la distorsion totale qui résulterait de l'indisponibilité de la zone ZOI donnée pour son décodage, en tenant compte non seulement de la valeur de la zone ZOI proprement dite (telle qu'exprimée par le champ de distorsion) mais en tenant compte également de la distorsion produite en raison de l'indécodabilité d'autres parties du flux binaire comprimé qui dépendent de la zone ZOI. La distorsion totale associée à différentes zones ZOI fournit une mesure utile de l'importance relative des différentes zones ZOI. Quand les deux champs sont utilisés, ils utilisent la même expression mathématique pour la distorsion, telle que signalée par le champ de distorsion.

5.7.3.3 Champ de débit binaire

Le champ de débit binaire sert à spécifier la zone protégée dans le domaine des coefficients d'ondelette. Il identifie les plans de bit de plus fort poids (MSB) dont le débit comprimé est spécifié par ce champ. Les bits MSB sont sélectionnés au moyen du processus d'optimisation de la distorsion en débit qui est spécifié dans la Partie 1. Par exemple, si la valeur du débit binaire est 2,5, la zone protégée contient les bits MSB de tous les coefficients d'ondelette dont le débit comprimé est de 2,5 bits par pixel. La syntaxe du champ de débit binaire est représentée dans la Figure 18 et dans le Tableau 18. Le débit binaire spécifié est donné par:

$$R = I_R + F_R/16$$

Par exemple, un débit binaire égal à 0 est représenté par $I_R = 0$ et $F_R = 0$; une valeur de débit binaire de 2,5 est représentée par $I_R = 2$ et $F_R = 8$.

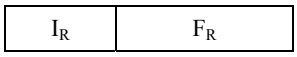


Figure 18 – Syntaxe du champ de débit binaire

I_R: partie entière du débit binaire spécifié.

F_R: partie fractionnaire du débit binaire spécifié.

Tableau 18 – Valeurs paramétriques du champ de débit binaire

Paramètre	Longueur (bits)	Valeurs
I_R	4	0 ... 15
F_R	4	0 ... 15

5.7.4 Relation entre paramètres multiples

5.7.4.1 Relation globale

Quand la classe de description associée à l'image possède de multiples champs activés simultanément, la zone résultante doit être l'intersection de ces champs. Par exemple, une zone pourrait spécifier le plus bas niveau de résolution dans le 2^e pavé. La réunion des champs peut être spécifiée par l'utilisation de multiples sous-zones dans la zone ZOI.

La classe de description non associée à l'image peut également avoir de multiples champs activés simultanément. Quand cela se produit, les modes pour les divers champs paramétriques doivent avoir le même nombre d'items (une exception à cette règle est décrite ci-dessous) et ces items doivent correspondre les uns avec les autres de façon biunivoque. Par exemple, si la zone utilise des étendues d'octet et des étendues de paquet, chacune devrait avoir le même nombre d'items d'étendue, la première étendue d'octet correspondant à la première étendue de paquet et ainsi de suite.

Il y a une exception à la règle ci-dessus, qui prescrit le même nombre d'items pour chaque champ: elle se produit quand un des champs f1 contient 1 item qui spécifie une étendue d'items contenant N éléments (comme décrit par l'étendue de mode dans le § 5.7.6) et quand un autre champ f2 est spécifié par une liste de N items. Dans ce cas, le champ f1, qui contient seulement 1 item (l'étendue) est interprété comme étant une liste de N items qui, spécifiés par l'étendue contenue dans le champ f1, doivent correspondre de façon biunivoque aux N items énumérés dans le champ f2. Une étendue d'items peut donc être associée soit à un unique item ou à de multiples items (une étendue pour chaque item qu'elle contient).

5.7.4.2 Exemples

Comme décrit dans la Figure 11, la structure de la classe de description de zone peut avoir de multiples champs activés simultanément, où N champs sont des descriptions associées à l'image (D_i^1, D_i^2, …, D_i^N) et où M champs sont des descriptions non associées à l'image (D_n^1, D_n^2, …, D_n^M). La sémantique peut être interprétée comme suit: $\{D_i^1 \cap D_i^2 \cap \ldots \cap D_i^N\} = D_n^1 = D_n^2 = \ldots = D_n^M$, c'est-à-dire que l'intersection des N descriptions associées à l'image correspondent à chacune des M descriptions non associées à l'image. En outre, les M descriptions non associées à l'image correspondent les unes avec les autres. Cette relation est également illustrée par les trois exemples ci-dessous.

Dans le premier exemple, la description de zone comporte deux descriptions associées à l'image: l'une pour la résolution 2 et l'autre pour la couche 3. Dans ce cas, les données influencées sont l'intersection de la résolution 2 et de la couche 3, comme illustré dans la Figure 19.

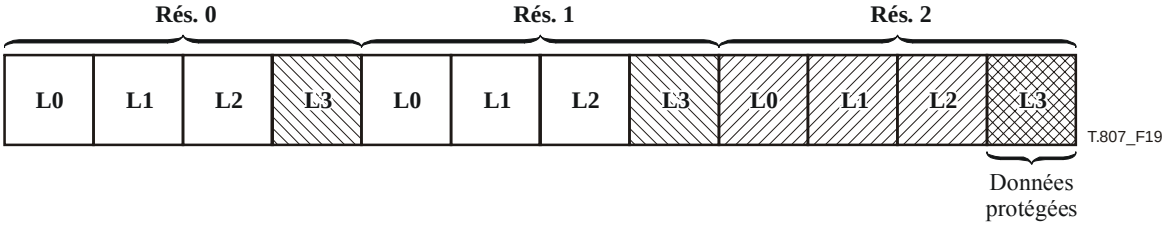


Figure 19 – Exemple de zone ZOI utilisant des descriptions associées à l'image

Dans le second exemple, la description de zone comporte deux descriptions associées à l'image (qui sont la résolution 2 et la couche 3) et une description non associée à l'image (qui est l'étendue de paquet de 80 à 100). Dans ce cas, les données influencées sont l'intersection de la résolution 2 et de la couche 3. Par ailleurs, cela indique que les données influencées sont contenues dans des paquets allant de 80 à 100.

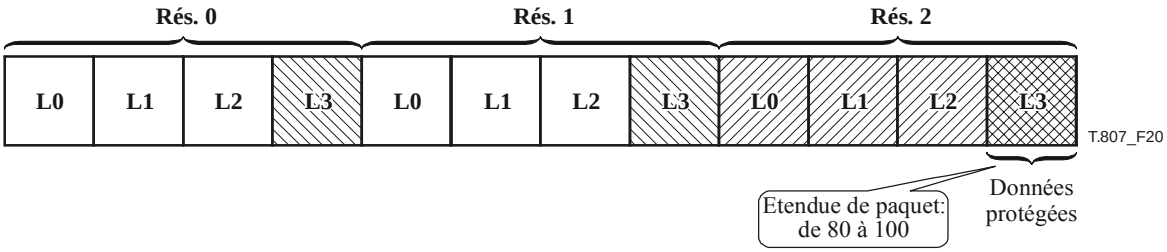


Figure 20 – Exemple de zone ZOI utilisant des descriptions associées et non associées à l'image

Dans le troisième exemple, la description de zone comporte deux descriptions associées à l'image (la résolution 2 et la couche 3) et deux descriptions non associées à l'image (l'étendue de paquet de 80 à 100 et l'étendue d'octet de 856 à 1250). Une fois de plus, les données influencées sont l'intersection de la résolution 2 et de la couche 3 tandis que les données influencées sont contenues dans des paquets allant de 80 à 100. Par ailleurs, ces paquets et la zone influencée sont situés dans l'étendue d'octet de 856 à 1250.

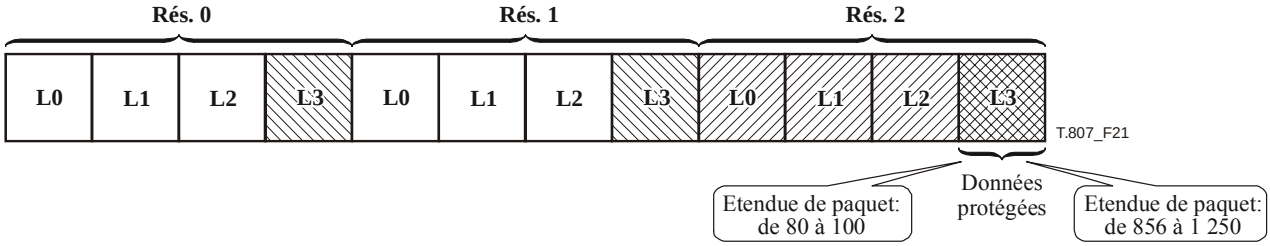


Figure 21 – Second exemple de zone ZOI utilisant des descriptions associées et non associées à l'image

5.7.5 Protection de toutes les données qui suivent le marqueur SEC

L'analyse qui précède est largement appliquée à la prise en charge de services de protection pour le flux à codage JPEG 2000. Cependant, de nombreux éléments de l'en-tête principal, y compris la signalisation JPSEC, devraient également être protégés; d'autre part, la zone ZOI et les méthodes de protection peuvent également être utilisées à cette fin.

Spécifiquement, le mode d'étendue d'octet de la classe de description non associée à l'image peut servir à spécifier qu'un outil JPSEC devrait être appliqué à toutes les données qui suivent le marqueur SEC. Comme décrit ci-dessus, le premier octet de l'en-tête de marqueur SEC est l'octet 1 pour indexer l'étendue d'octet. Les données qui suivent le marqueur SEC et qui peuvent être protégées contiennent le segment marqueur SEC et la plus grande partie de l'en-tête principal. Noter que la totalité de l'en-tête principal JPEG 2000, sauf pour le segment marqueur SIZ, peut être déplacée après le marqueur SEC et peut donc être protégée au moyen de la méthode qui précède. Si le segment marqueur SIZ du codage JPEG 2000 doit être protégé, cette protection doit être effectuée à un niveau supérieur, p. ex. dans la couche des formats de fichier.

Les outils JPSEC permettant de protéger le segment marqueur SEC devraient généralement être les premiers outils dans le segment marqueur SEC. Cela permet au consommateur de restituer d'abord les données du segment marqueur SEC, qui peuvent ensuite servir à traiter le reste du flux codé.

5.7.6 Syntaxe du paramètre de description de zone (Pzoi)

La Figure 22 montre la syntaxe du paramètre de description de zone ZOI.

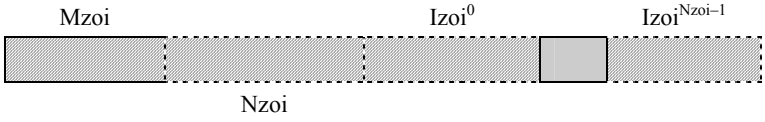


Figure 22 – Syntaxe du paramètre de description de zone ZOI

Mzoi: mode de description de zone ZOI. Ce champ utilise la structure de segment FBAS.

Nzoi: nombre d'items Izoi. Ce champ utilise la structure de segment RBAS.

Izoi^{i}: item.

Tableau 19 – Valeurs du paramètre Pzoi^{i}

Paramètre	Longueur (bits)	Valeurs
Mzoi	Variable (FBAS)	Voir Tableau 20
Nzoi	0 8 + 8 * n (RBAS)	Si la position binaire 2 de Mzoi est 0. 2 ... (2^{7+7*n} – 1)
Izoi^{i}	Variable	Dépend du mode spécifié dans Mzoi

Tableau 20 – Valeurs du paramètre Mzoi

Numéro de bit de segment FBAS	Valeurs (bits)	Sémantique
1	0	Les zones spécifiées sont influencées par l'outil JPSEC
	1	Le complément de zones spécifiées est influencé
2	0	Un item unique est spécifié
	1	De multiples items sont spécifiés
3, 4	00	Mode rectangulaire. Région rectangulaire dans laquelle la première paire de valeurs spécifie le coin supérieur gauche et où la seconde paire de valeurs spécifie le coin inférieur droit de façon que ces deux coins soient réunis. Pour chaque coin, la première valeur doit être la position horizontale et la seconde valeur doit être la position verticale. L'indexation doit commencer à 0 et doit utiliser la grille de référence définie dans la Partie 1 de la norme JPEG 2000.
	01	Mode d'étendue. Etendue de valeurs où la première valeur spécifie l'indice de départ et où la seconde valeur spécifie le dernier indice, réunis l'un à l'autre.
	10	Mode indiciel. Spécifie une (des) valeur(s) unique(s).
	11	Mode maximal. Spécifie la valeur maximale.
5, 6	00	$Izoi^i$ utilise des entiers de 8 bits
	01	$Izoi^i$ utilise des entiers de 16 bits
	10	$Izoi^i$ utilise des entiers de 32 bits
	11	$Izoi^i$ utilise des entiers de 64 bits
7, 8	00	$Izoi^i$ est décrit dans une seule dimension
	10	$Izoi^i$ est décrit dans deux dimensions
	01	$Izoi^i$ est décrit dans l'ordre trois dimensions
9	0	Le mode de décalage de longueur n'est pas utilisé
	1	Le mode de décalage de longueur est utilisé et spécifie le décalage initial par rapport aux longueurs des octets contigus qui suivent. L'existence de ce fanion doit avoir priorité sur les modes spécifiés dans les bits 3 et 4.
		Toutes les autres valeurs sont réservées

Quand des balises indicielles TRLCP sont utilisées, leur longueur est définie par le paramètre P_{TRLCP} comme spécifié dans le Tableau 4. Dans ce cas, les bits 5 et 6 du paramètre M_{ZOI} sont supplantés.

Le mode de décalage de longueur peut servir à représenter efficacement une série de segments consécutifs, p. ex., une série d'étendues d'octet consécutives. La première valeur spécifie le décalage initial, les valeurs suivantes spécifient la longueur de chaque segment consécutif. Si ce champ sert à représenter n segments, alors le paramètre Nzoi devrait être réglé à n + 1.

5.8 Syntaxe du modèle de méthode de protection (T)

5.8.1 Généralités

Les modèles de méthode de protection contiennent des paramètres pour les outils JPSEC spécifiquement décrits dans le § 5.6.1. Par exemple, ils sont utilisés dans les outils JPSEC normatifs décrits dans le § 5.6.2. De même, ils peuvent être utilisés dans les outils JPSEC non normatifs décrits dans le § 5.6.3. Il y a trois types de modèle de méthode de protection: le modèle de déchiffrement, le modèle d'authentification et le modèle de hachage. Le modèle utilisé par un outil JPSEC normatif est spécifié par son identificateur comme représenté dans le Tableau 6 et de nouveau dans le Tableau 21 ci-dessous avec des références aux paragraphes appropriés où ils sont définis.

Comme décrit dans le § 5.6.2, le modèle de méthode de protection T, associé à un domaine de traitement PD, à une granularité G et à une liste de valeurs V d'outil JPSEC, décrit comment un outil JPSEC est appliqué.

Tableau 21 – Valeurs du numéro d'identification d'un modèle (ID_T)

Valeurs	Modèle de méthode de protection
0	Réservé
1	Modèle de déchiffrement. Voir § 5.8.2.
2	Modèle d'authentification. Voir § 5.8.3.
3	Modèle de hachage. Voir § 5.8.4.
4	Outil NEANT
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.2 Modèle de déchiffrement ($T = T_{decry}$, si $t = 0$ et $ID = 1$)

Le modèle de déchiffrement, T_{decry}, sert à communiquer au déchiffreur la façon de déchiffrer le flux codé reçu. La Figure 23 montre la syntaxe du modèle de déchiffrement. Le Tableau 22 montre les longueurs et valeurs des symboles et paramètres pour le modèle de déchiffrement.

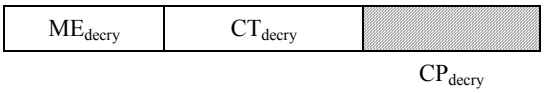


Figure 23 – Syntaxe du modèle de déchiffrement

ME_{decry}: fanion de fausse émulation de marqueur qui indique si une fausse émulation de marqueur s'est produite dans les données chiffrées. Une fausse émulation de marqueur peut affecter défavorablement la conformité à la Partie 1 de la norme JPEG 2000 sur les décodeurs. Ce champ utilise la structure de segment FBAS;

CT_{decry}: identification du type de chiffrement;

CP_{decry}: paramètre de chiffrement.

Tableau 22 – Valeurs paramétriques du modèle de déchiffrement

Paramètre	Longueur (bits)	Valeurs
ME_{decry}	8 + 8 * n (FBAS)	Tableau 23
CT_{decry}	16	Tableau 24
CP_{decry}	Variable	Si $CT_{decry} < 0x6000$, voir § 5.8.2.1. Si $0x6000 \leq CT_{decry} < 0xC000$, voir § 5.8.2.2. Si $CT_{decry} \geq 0xC000$, voir § 5.8.2.3.

Tableau 23 – Valeurs du fanion d'émulation de marqueur (ME_{decry})

Valeurs	Type de méthode
01xx xxxx	Les données chiffrées ne contiennent pas de fausse émulation de marqueur.
00xx xxxx	Sinon
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

La valeur par défaut du fanion d'émulation de marqueur est 0. Ce fanion peut être réglé à 1 afin d'indiquer que les données chiffrées JPSEC ne contiennent pas de fausse émulation de marqueur. Un créateur JPSEC peut décider de laisser ce fanion à sa valeur par défaut de 0.

Tableau 24 – Valeurs de l'identificateur de chiffrement (CT_{decry})

Valeurs	Type de chiffrement
0 ... 0x5FFF	Chiffrement par blocs (Voir Tableau 25)
0x6000 ... 0xBFFF	Chiffrement par flux (Voir Tableau 26)
0xC000 ... 0xFFFF	Chiffrement asymétrique (Voir Tableau 27)

Tableau 25 – Valeurs de l'identificateur de chiffrement par blocs valeurs (CT_{decry})

Valeurs	Type de chiffrement
0x0000	NULL (aucun chiffrement)
0x0001	AES (ISO/CEI 18033-3)
0x0002	TDEA (ISO/CEI 18033-3)
0x0003	MISTY1 (ISO/CEI 18033-3)
0x0004	Camellia (ISO/CEI 18033-3)
0x0005	CAST-128 (ISO/CEI 18033-3)
0x0006	SEED (ISO/CEI 18033-3)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

Tableau 26 – Valeurs de l'identificateur de chiffrement par flux (CT_{decry})

Valeurs	Type de chiffrement
0x6000	SNOW 2 (ISO/CEI 18033-4)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

Tableau 27 – Valeurs de l'identificateur de chiffrement asymétrique (CT_{decry})

Valeurs	Type de chiffrement
0xC000	RSA-OAEP (ISO/CEI 18033-2)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.2.1 Modèle de chiffrement par blocs (CP_{decry} pour chiffrement par blocs)

Le modèle de chiffrement par blocs sert à communiquer au déchiffreur de blocs la façon de déchiffrer le flux codé reçu. La Figure 24 montre le mode de chiffrement par blocs, le mode de bourrage, la longueur de bloc et les informations sur les clés.

Certains modes de chiffrement par blocs peuvent utiliser des vecteurs d'initialisation. Pour ces modes, les vecteurs d'initialisation de l'outil sont spécifiés au moyen du champ de granularité (G) de l'outil, décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. Spécifiquement, les vecteurs d'initialisation ne servent qu'aux modes avec ID $M_{bc} > 0x80$, p. ex. les modes CBC, CFB, OFB, CTR. Dans le cas du mode CTR, ce n'est pas vraiment un vecteur d'initialisation (IV) mais un *compteur*. La longueur du vecteur d'initialisation spécifiée dans la liste de valeurs V doit être réglée à la longueur de bloc SIZ_{bc}.

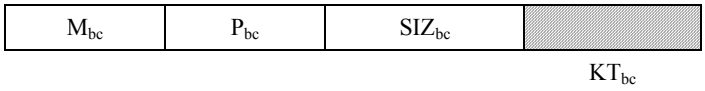


Figure 24 – Syntaxe du modèle de chiffrement par blocs

M_{bc}: mode de chiffrement par blocs. Le premier bit indique l'utilisation de vecteurs d'initialisation avec cet outil. Si $M_{bc} < 0x8$, des vecteurs d'initialisation ne sont pas utilisés, sinon une ou plusieurs valeurs de vecteur d'initialisation sont requises pour ce mode.

P_{bc}: mode de bourrage.

SIZ_{bc}: longueur de bloc en octets.

KT_{bc}: modèle de clé (voir § 5.8.5) qui contient des informations sur les clés utilisées pour le chiffrement par blocs.

Tableau 28 – Valeurs du modèle de chiffrement par blocs

Paramètre	Longueur (bits)	Valeurs
M_{bc}	6	Tableau 29
P_{bc}	2	Tableau 30
SIZ_{bc}	8	1 ... 256
KT_{bc}	Variable	Voir § 5.8.5

Tableau 29 – Valeurs du mode de chiffrement par blocs (M_{bc})

Valeurs	Type de mode
0	Réservé
0x xxxx	Modes qui sont utilisés sans vecteur d'initialisation
1x xxxx	Modes qui sont utilisés avec un vecteur d'initialisation
x0 xxxx	Bits non justifiés par bourrage
x1 xxxx	Bits justifiés par bourrage
0x 0001	ECB (ISO/CEI 10116)
1x 0010	CBC (ISO/CEI 10116)
1x 0011	CFB (ISO/CEI 10116)
1x 0100	OFB (ISO/CEI 10116)
1x 0101	CTR (ISO/CEI 18033-2)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

NOTE 1 – Des implémentations attentives sont requises dans tous les modes, parce que des implémentations impropres peuvent conduire à des vulnérabilités. Noter que même une implémentation correcte du mode ECB présente des fuites d'informations quand des blocs identiques apparaissent. Des directives sont contenues dans l'ISO/CEI 10116.

NOTE 2 – Les valeurs indiquées dans le Tableau 30 ne s'appliquent que lorsque M_{bc} – dans le Tableau 29 – spécifie que les bits sont justifiés par bourrage. Quand les bits ne sont pas justifiés par bourrage, P_{bc} doit être réglé à 00.

Tableau 30 – Mode de bourrage pour chiffrement par blocs (P_{bc})

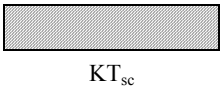
Valeurs	Type de bourrage
00	Vol de cryptogramme (RFC 2040)
01	Bourrage PKCS#7 (PKCS#7)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

NOTE 3 – Lors de l'utilisation du bourrage, la conception du système doit être soigneusement élaborée afin d'éviter d'éventuelles vulnérabilités de sécurité, comme des attaques par chiffre choisi.

5.8.2.2 Modèle de chiffrement par flux (CP_{decry} pour chiffrement par flux)

Le modèle de chiffrement par flux sert à communiquer au déchiffreur de flux la façon de déchiffrer le flux codé reçu. La Figure 25 montre la syntaxe du modèle de chiffrement par flux. Le Tableau 31 montre les valeurs du modèle de chiffrement par flux.

Les vecteurs d'initialisation du chiffrement par flux sont spécifiés au moyen du champ de granularité (G) de l'outil décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. La longueur du vecteur d'initialisation spécifiée dans la liste de valeurs V doit être réglée à longueur de clé définie dans le modèle d'informations de clé KT_{sc}.



KT_{sc}

Figure 25 – Syntaxe du modèle de chiffrement par flux

KT_{sc}: modèle d'informations de clé (voir § 5.8.5) qui contient les informations sur les clés utilisées par le chiffrement par flux.

Tableau 31 – Valeurs du modèle de chiffrement par flux

Paramètre	Longueur (bits)	Valeurs
KT_{sc}	Variable	Voir § 5.8.5

5.8.2.3 Modèle de chiffrement asymétrique (CP_{decry} pour chiffrement asymétrique)

Le modèle de chiffrement asymétrique sert à communiquer, au déchiffreur de chiffrement asymétrique, la façon de déchiffrer le flux codé reçu. La Figure 26 montre la syntaxe du modèle de chiffrement asymétrique. Le Tableau 32 montre les valeurs du modèle de chiffrement asymétrique.

Pour les outils qui utilisent le modèle de chiffrement asymétrique, le champ de granularité (G) de l'outil spécifie la granularité avec laquelle chiffrement est appliqué. Cependant, le champ de liste de valeurs (V) ne sert pas à représenter de quelconques valeurs. Le nombre d'éléments (N_v) contenus dans le champ de liste de valeurs doit donc être réglé à 0.

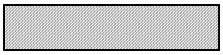


Figure 26 – Syntaxe du modèle de chiffrement asymétrique

KT_{sy}: modèle d'informations de clé (voir § 5.8.5) qui contient les informations sur les clés utilisées par le chiffrement asymétrique.

Tableau 32 – Valeurs du modèle de chiffrement asymétrique

Paramètre	Longueur (bits)	Valeurs
KT_{sy}	Variable	Voir § 5.8.5

5.8.3 Modèle d'authentification ($T = T_{auth}$, si t = 0 et ID = 2)

Le modèle d'authentification, T_{auth}, sert à communiquer au vérificateur la façon de vérifier l'authenticité du flux codé reçu. Il y a trois classes générales de méthode d'authentification: l'authentification fondée sur un hachage, l'authentification fondée sur un algorithme de chiffrement et les signatures numériques. Par ailleurs, la méthode fondée sur un hachage et la méthode fondée sur un algorithme de chiffrement sont toutes les deux désignées généralement par le terme de *code d'authentification de message* (MAC). Leurs valeurs calculées, utilisées pour l'authentification, sont généralement appelées *valeurs de code MAC*. La syntaxe du modèle d'authentification est représentée dans la Figure 27. Le Tableau 33 montre les longueurs et valeurs des symboles et paramètres pour le modèle d'authentification.

Dans de nombreuses applications de sécurité, l'authentification est le plus important service de sécurité. Même quand la confidentialité est le service de sécurité recherché, celui-ci devrait être augmenté par l'authentification afin d'empêcher des attaques. En particulier, il est recommandé d'authentifier des parties du segment marqueur SEC. En outre, l'authentification doit être effectuée aussi bien sur les paramètres du modèle d'authentification (T_{auth}) que sur le message à authentifier. Spécifiquement, la zone d'influence doit spécifier qu'aussi bien le contenu que les paramètres du modèle d'authentification (T_{auth}) doivent être authentifiés.

Figure 27 – Syntaxe du modèle d'authentification

M_{auth}: méthode d'authentification.

P_{auth}: paramètres d'authentification.

Tableau 33 – Valeurs paramétriques du modèle d'authentification

Paramètre	Longueur (bits)	Valeurs
M_{auth}	8	Tableau 34
P_{auth}	Variable	If M_{auth} = 0, voir § 5.8.3.1 If M_{auth} = 1, voir 5.8.3.2 If M_{auth} =2, voir 5.8.3.3

Tableau 34 – Méthodes d'authentification (M_{auth})

Valeurs	Méthode
0	Code MAC fondé sur hachage
1	Code MAC fondé sur chiffrement
2	Signature numérique
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.3.1 Authentification fondée sur un hachage (P_{auth} pour code MAC fondé sur hachage)

Le code MAC d'authentification fondée sur un hachage sert à communiquer au vérificateur la façon de vérifier l'authenticité du flux codé reçu. La Figure 28 montre la syntaxe du modèle d'authentification fondée sur un hachage syntaxe et le Tableau 35 en montre les valeurs paramétriques.

Les valeurs de code MAC sont spécifiées au moyen du champ de granularité (G) de l'outil décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. La longueur de la valeur de code MAC spécifiée dans la liste de valeurs V doit être réglée à la longueur de code MAC définie par le paramètre SIZ_{HMAC}.

Figure 28 – Modèle d'authentification fondée sur un hachage

M_{HMAC}: identificateur de la méthode d'authentification fondée sur un hachage.

H_{HMAC}: identificateur de la fonction de hachage.

KT_{HMAC}: modèle de clé.

SIZ_{HMAC}: longueur de code MAC (bits)

Tableau 35 – Valeurs paramétriques du modèle d'authentification fondée sur un hachage

Paramètre	Longueur (bits)	Valeurs
M_{HMAC}	8	Tableau 36
H_{HMAC}	8	Tableau 37
KT_{HMAC}	Variable	Voir § 5.8.5
SIZ_{HMAC}	16	0-65535

Tableau 36 – Identificateur de la méthode d'authentification fondée sur un hachage (M_{HMAC})

Valeurs	Méthode d'authentification fondée sur un hachage
0	Réservé
1	HMAC (ISO/CEI 9797-2)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

Tableau 37 – Identificateur de la fonction de hachage (H_{HMAC})

Valeurs	Fonction de hachage
0	Réservé
1	SHA-1 (ISO/CEI 10118-3)
2	RIPEMD-128 (ISO/CEI 10118-3)
3	RIPEMD-160 (ISO/CEI 10118-3)
4	MASH-1 (ISO/CEI 10118-4)
5	MASH-2 (ISO/CEI 10118-4)
6	SHA-224 (ISO/CEI 10118-3)
7	SHA-256 (ISO/CEI 10118-3)
8	SHA-384 (ISO/CEI 10118-3)
9	SHA-512 (ISO/CEI 10118-3)
10	WHIRLPOOL (ISO/CEI 10118-3)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

Noter que si le paramètre SIZ_{HMAC} est inférieur à la longueur nominale du hachage, alors il s'agit de la version tronquée correspondant aux premiers bits SIZ_{HMAC} du hachage.

5.8.3.2 Modèle d'authentification fondé sur un algorithme de chiffrement (P_{auth} pour code MAC fondé sur chiffrement)

Le code MAC d'authentification fondée sur un algorithme de chiffrement sert à communiquer au vérificateur la façon de vérifier l'authenticité du flux codé reçu. La Figure 29 est son modèle et le Tableau 38 montre la longueur de clé et l'adressage dispersé sur clés calculées. Un exemple de système d'authentification fondé sur un algorithme de chiffrement est le code CBC-MAC. Dans ces techniques de chiffrement par blocs pour l'authentification, le vecteur d'initialisation est de longueur égale à un seul bloc et de valeur 0. La longueur de bloc est la valeur par défaut pour le chiffrement par blocs. Noter que si le paramètre SIZ_{CMAC} est inférieur à la longueur nominale du code MAC d'authentification fondée sur un algorithme de chiffrement, alors il s'agit de la version tronquée correspondant aux premiers bits SIZ_{CMAC} du code MAC.

Noter que si le nombre de bits de données n'est pas un multiple de la longueur du bloc de chiffrement, alors le bloc d'entrée final sera un bloc de données partiel, justifié à gauche, avec des zéros adjoints de façon à former un bloc de chiffrement complet. Noter également que le code CBC-MAC ne doit être appliqué qu'aux données de longueur fixe et connue.

Les valeurs de code MAC sont spécifiées au moyen du champ de granularité (G) de l'outil décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. La longueur de la valeur de code MAC spécifiée dans la liste de valeurs V doit être réglée à la longueur de code MAC définie par SIZ_{CMAC}.

Figure 29 – Syntaxe du modèle d'authentification fondé sur un algorithme de chiffrement

CA_{CMAC}: méthode d'authentification fondée sur un algorithme de chiffrement.

C_{CMAC}: valeur de l'identificateur de chiffrement par blocs.

KT_{CMAC}: modèle de clé.

SIZ_{CMAC}: longueur du code MAC (bits).

Tableau 38 – Valeurs du modèle de code MAC

Paramètre	Longueur (bits)	Valeurs
CA_{CMAC}	8	Tableau 39
C_{CMAC}	8	Tableau 25
KT_{CMAC}	Variable	voir § 5.8.5
SIZ_{CMAC}	16	0 ... 65535

Tableau 39 – Méthode d'authentification fondée sur un algorithme de chiffrement (C_{CMAC})

Valeurs	Méthode
0	CBC-MAC - Algorithme MAC 1 (ISO/CEI 9797-1)
1	CBC-MAC - Algorithme MAC 2 (ISO/CEI 9797-1)
2	CBC-MAC - Algorithme MAC 3 (ISO/CEI 9797-1)
3	CBC-MAC - Algorithme MAC 4 (ISO/CEI 9797-1)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.3.3 Modèle de signature numérique (P_{auth} pour signatures numériques)

La signature numérique sert à communiquer au vérificateur la façon de vérifier l'authenticité du flux codé reçu ainsi que l'identité de l'expéditeur aux fins de son identification comme de sa non-répudiation. La Figure 30 définit son modèle et le Tableau 40 en énumère les valeurs.

Les signatures numériques sont spécifiées au moyen du champ de granularité (G) de l'outil décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. La longueur de la valeur des signatures numériques, spécifiée dans la liste de valeurs V, doit être réglée de façon à contenir la longueur définie par le paramètre SIZ_{DS}. Etant donné que la longueur de la liste de valeurs est représentée en octets plutôt qu'en bits, cette longueur devrait être le nombre minimal d'octets qui peuvent contenir le paramètre SIZ_{DS}. Chaque valeur devrait être représentée avec les bits de plus faible poids et les bits MSB supplémentaires doivent être réglés à 0.

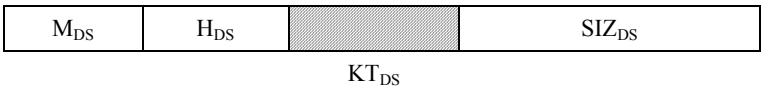


Figure 30 – Syntaxe du modèle de signature numérique

M_{DS}: méthode de signature numérique

H_{DS}: fonction de hachage

KT_{DS}: modèle de clé (voir § 5.8.5) qui contient toutes les informations associées à la clé publique ou le certificat requis afin de vérifier la signature numérique.

SIZ_{DS}: longueur de signature numérique (bits)

Tableau 40 – Valeurs du modèle de signature numérique

Paramètre	Longueur (bits)	Valeurs
M_{DS}	8	Tableau 41
H_{DS}	8	Tableau 37
KT_{DS}	Variable	Voir § 5.8.5
SIZ_{DS}	16	0 ... 65535

Tableau 41 – Méthodes de signature numérique (M_{DS})

Valeurs	Méthode
1	RSA (ISO/CEI 14888-2)
2	Rabin (ISO/CEI 14888-2)
3	DSA (ISO/CEI 14888-3)
4	ECDSA (ISO/CEI 14888-3)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.4 Modèle de hachage ($T = T_{hash}$, si t = 0 et ID = 3)

Le modèle de hachage, T_{hash}, sert à communiquer les paramètres servant à calculer le hachage. Le Tableau 42 montre les longueurs et valeurs des symboles et paramètres du modèle de hachage.

Noter que, contrairement au modèle d'authentification fondée sur un hachage analysé dans le § 5.8.3.1, qui implique l'utilisation d'un hachage et d'une clé secrète, ce modèle de hachage n'utilise pas de clé. Bien que ce modèle de hachage puisse servir à détecter une erreur accidentelle ou une modification accidentelle des données, il n'empêche pas une altération malveillante des données. Afin d'empêcher une altération malveillante des données, un modèle d'authentification doit être utilisé, car la clé secrète utilisée par le modèle d'authentification empêche les données d'être altérées sans avoir été préalablement découvertes.

Les valeurs de hachage sont spécifiées au moyen du champ de granularité (G) de l'outil décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V) décrit dans le § 5.11. La longueur de la valeur de hachage spécifiée dans la liste de valeurs V doit être réglée à longueur de valeur de hachage définie par SIZ_{hash}.

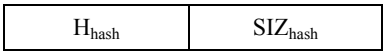


Figure 31 – Syntaxe du modèle de hachage

H_{hash}: identificateur de la fonction de hachage.

SIZ_{hash}: longueur de la valeur de hachage (octets).

Tableau 42 – Valeurs paramétriques du modèle de hachage

Paramètre	Longueur (bits)	Valeurs
H_{hash}	8	Tableau 37
SIZ_{hash}	8	0 ... 255

5.8.5 Modèle d'informations de clé (KT)

Le modèle d'informations de clé sert à communiquer les informations sur les clés. La Figure 32 définit son modèle et le Tableau 43 en énumère les valeurs.

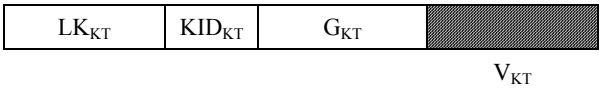


Figure 32 – Syntaxe du modèle d'informations de clé

LK_{KT}: longueur de clé en bits.

KID_{KT}: identificateur d'informations sur les clés, qui indique la signification des valeurs contenues dans la liste de valeurs V_{KT}. Dans le modèle de déchiffrement, cette valeur devrait être réglée à 2 (identificateur URI permettant d'extraire la clé secrète). Dans le cas de signature numérique, la valeur de ce champ est libre.

G_{KT}: champ de granularité afin de représenter la granularité avec laquelle les informations sur les clés sont modifiées.

V_{KT}: champ de liste de valeurs afin de représenter la liste évolutive d'informations sur les clés.

Noter que, dans le cas d'une clé secrète (modèle de déchiffrement), la clé publique et le certificat n'ont aucune signification: le modèle de clé devrait contenir certaines informations sur l'emplacement de la clé (p. ex. l'identificateur URI).

Les informations sur les clés peuvent être représentées par une ou plusieurs valeurs au moyen du champ de granularité (G_{KT}) décrit dans le § 5.10 et au moyen du champ de liste de valeurs (V_{KT}) décrit dans le § 5.11. Les deux champs (G_{KT} et V_{KT}) déterminent ensemble comment les valeurs de clé contenues dans la liste de valeurs (V_{KT}) sont appliquées aux données protégées d'image, comme décrit dans le § 5.10 et le § 5.11.

Les informations sur les clés contenues dans la liste de valeurs peuvent prendre les formes spécifiées dans le Tableau 44. Si $KID_{KT} = 1$, alors chaque valeur est spécifiée avec le modèle du certificat X.509 décrit dans le § 5.8.5.1. Si $KID_{KT} = 2$, alors chaque valeur est spécifiée avec un identificateur URI pour le certificat ou la clé secrète.

Tableau 43 – Valeurs du modèle de clé

Paramètre	Longueur (bits)	Valeurs
LK_{KT}	16	1 ... 65535
KID_{KT}	8	Tableau 44
G_{KT}	24	Voir § 5.10
V_{KT}	Variable	Voir § 5.11

Tableau 44 – Valeurs de l'identificateur d'informations sur les clés (KID_{KT})

Valeurs	Identificateur d'informations sur les clés
0	Réservé
1	Certificat X.509 (ISO/CEI 9594-8)
2	URI pour certificat ou clé secrète
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.8.5.1 Modèle du certificat X.509

Figure 33 – Syntaxe du certificat X.509

ER_{KT}: règle de codage pour certificat X.509.

$LCER_{KT}$: longueur du certificat X.509 (CERKT) en octets.

CER_{KT}: certificat X.509.

Tableau 45 – Valeurs du certificat X.509 (KI_{KT} si $KID_{KT} = 2$)

Paramètre	Longueur (bits)	Valeurs
ER_{KT}	8	0 ... 255 (voir Tableau 46)
$LCER_{KT}$	16	1 ... 65535
CER_{KT}	Variable	–

Tableau 46 – Valeurs de règle de codage (ER_{KT})

Valeurs	Identificateur de règle de codage
0	Réservé
1	DER (RFC 3217)
2	BER (RFC 3394)
	Toutes les autres valeurs sont réservées pour utilisation par l'ISO

5.9 Syntaxe du domaine de traitement (PD)

La syntaxe du domaine de traitement sert à indiquer le domaine auquel l'outil JPSEC est appliqué. Les domaines possibles sont les suivants: celui des pixels, celui des coefficients d'ondelette, celui des coefficients d'ondelette quantifiés et celui des flux codés.

Figure 34 – Syntaxe du domaine de traitement

PD: domaine de traitement. Ce champ utilise la structure de segment FBAS.

F_{PD}: champ du domaine de traitement afin d'offrir des informations plus détaillées sur le domaine de traitement. Ce champ utilise la structure de segment FBAS.

Tableau 47 – Paramètres du domaine de traitement

Paramètre	Longueur (bits)	Valeurs
PD	Variable (FBAS)	Voir Tableau 48
F_{PD}	Variable (FBAS)	Dans le domaine des coefficients d'ondelette et dans le domaine des coefficients d'ondelette quantifiés, Voir Tableau 49 Dans le domaine du flux codé, Voir Tableau 50

Tableau 48 – Valeurs paramétriques du domaine de traitement (PD)

Numéro du bit de segment FBAS	Valeurs	Sémantique
1	1	Domaine des pixels. La méthode de protection est appliquée aux éléments d'image (pixels).
	0	Sinon
2	1	Domaine des coefficients d'ondelette: la méthode de protection est appliquée aux coefficients d'ondelette.
	0	Sinon
3	1	Domaine des coefficients d'ondelette quantifiés: la méthode de protection est appliquée aux coefficients d'ondelette quantifiés.
	0	Sinon
4	1	Domaine du flux codé: la méthode de protection est appliquée au flux codé issu du codeur arithmétique.
	0	Sinon

Noter que le champ PD doit avoir un et un seul bit réglé à 1, parce que chaque outil JPSEC n'est applicable qu'à 1 domaine.

Dans le domaine des éléments d'image (pixels), dans le domaine des coefficients d'ondelette et dans le domaine des coefficients d'ondelette quantifiés, les données bidimensionnelles doivent être transformées de façon à être unidimensionnelles afin d'appliquer les outils de sécurité. Cette transformation doit être effectuée par balayage des données bidimensionnelles d'image dans l'ordre matriciel.

Tableau 49 – Valeurs paramétriques du champ de domaine de traitement (F_{PD}) dans le domaine des coefficients d'ondelette et dans le domaine des coefficients d'ondelette quantifiés

Numéro du bit de segment FBAS	Valeur	Sémantique
1	0	La méthode de protection est appliquée aux bits de signe
	1	La méthode de protection est appliquée aux bits de plus fort poids

Tableau 50 – Valeurs paramétriques du champ de domaine de traitement (F_{PD}) dans le domaine du flux codé

Numéro du bit de segment FBAS	Valeur	Sémantique
1	0	La méthode de protection est appliquée aussi bien à l'en-tête qu'au corps de paquet
	1	La méthode de protection n'est appliquée qu'au corps de paquet

Le champ (F_{PD}) sert à offrir d'autres informations sur le domaine de traitement. Avec une valeur différente du domaine PD, ce champ (F_{PD}) a une sémantique différente. P. ex., dans le domaine des coefficients d'ondelette et dans le domaine des coefficients d'ondelette quantifiés, le premier bit de F_{PD} sert à indiquer si l'outil JPSEC est appliqué au bit de plus fort poids; dans le domaine du flux codé, le premier bit de F_{PD} sert à indiquer si l'outil JPSEC est appliqué seulement au corps de paquet ou à la fois à l'en-tête et au corps de paquet; dans le domaine des pixels, ce champ (F_{PD}) est réservé.

5.10 Syntaxe de granularité (G)

La granularité sert à indiquer l'unité de protection pour chaque méthode de protection. Le Tableau 53 définit des granularités possibles. La Figure 35 montre la syntaxe de granularité.

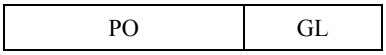


Figure 35 – Syntaxe de granularité

PO: ordre de traitement

GL: niveau de granularité

Tableau 51 – Valeurs paramétriques de la granularité (G)

Paramètre	Longueur (bits)	Valeurs
PO	16	Voir Tableau 52
GL	8	Voir Tableau 53

Tableau 52 – Valeurs de l'ordre de traitement (PO)

Valeurs MSB LSB	Ordre de traitement
0 000 000 000 000 000	Ordre spécifié par des paramètres de zone d'influence associée à une image
1 000 000 000 000 000	Ordre spécifié par un flux binaire de zone d'influence non associée à une image
1 000 000 000 000 001	Ordre spécifié par des paramètres de paquet de zone d'influence non associée à une image
0 000 001 010 011 100	Pavé-résolution-couche-composante-district
0 000 011 100 001 010	Composante de pavé-district-résolution-couche
0 000 010 001 011 100	Pavé-couche-résolution-composante-district
0 000 100 011 001 010	Pavé-district-composante-résolution-couche
0 000 001 100 011 100	Pavé-résolution-district-composante-couche
	Toutes les autres valeurs sont réservées

Tableau 53 – Valeurs du niveau de granularité (GL)

Valeurs MSB LSB	Granularité
0000 0000	Pavé
0000 0001	Elément de pavé
0000 0010	Composante
0000 0011	Niveau de résolution
0000 0100	Couche
0000 0101	District
0000 0110	Paquet
0000 0111	Sous-bande
0000 1000	Bloc de code
0000 1001	Aire totale identifiée dans la zone ZOI
1000 0000	Item identifié dans la zone d'influence non associée à l'image
1000 0001	Zone identifiée dans la zone d'influence non associée à l'image
	Toutes les autres valeurs sont réservées.

Afin de traiter la totalité de la zone spécifiée par ZOI, le niveau de granularité devrait être "zone identifiée dans la zone ZOI".

5.11 Syntaxe de liste de valeurs (V)

Le champ de liste de valeurs sert à spécifier des valeurs qui changent lorsque l'outil est appliqué et à spécifier la granularité de ce changement. Ce champ sert à signaler des valeurs changeantes telles que clés, vecteurs d'initialisation, valeurs de code MAC, signatures numériques et valeurs de hachage. Le champ de liste de valeurs spécifie d'abord le nombre de valeurs contenues dans la liste et la longueur de chaque valeur. Il énumère ensuite les valeurs proprement dites.

Comme analysé dans le § 5.6.2, pour les outils JPSEC normatifs le champ de liste de valeurs représente un paramètre différent pour chaque modèle. Dans le modèle de déchiffrement, ce champ représente les vecteurs d'initialisation IV_{bc} ou IV_{sc} selon qu'on utilise un chiffrement par blocs ou un chiffrement par flux. Dans le modèle d'authentification, ce champ représente la valeur de code MAC VAL_{MAC} pour l'authentification fondée sur un hachage ou sur un algorithme de chiffrement. Dans le modèle de signature numérique, ce champ représente la signature numérique SIG_{DS}. Dans le modèle de hachage, il représente la valeur de hachage HV_{hash}. Certains usages des modèles n'exigent pas que des valeurs soient spécifiées, p. ex., tous les modes de déchiffrement n'utilisent pas de vecteurs d'initialisation. Dans ces cas, le champ de liste de valeurs devrait mettre à zéro N_v et S_v de façon que la liste de valeurs VL ne contienne aucun élément. Si seule une valeur unique a besoin d'être spécifiée, p. ex., si une clé unique est utilisée dans toute l'image, alors N_v sera réglé à 1 de façon qu'une valeur unique soit contenue dans la liste de valeurs.

Figure 36 – Syntaxe du champ de liste de valeurs

N_V: nombre de valeurs contenues dans la liste de valeurs VL. Si $N_V = 0$, alors le champ se termine. Ce champ utilise la structure de segment RBAS.

S_V: longueur de chaque valeur contenue dans la liste de valeurs VL en octets. Ce champ utilise la structure de segment RBAS.

VL: liste de valeurs

Tableau 54 – Valeurs paramétriques du champ de liste de valeurs (V)

Paramètre	Longueur (bits)	Valeurs
N_V	16 + 8 * n (RBAS)	0 ... $(2^{15+7*n} - 1)$
S_V	8 + 8 * n (RBAS)	0 ... $(2^{15+7*n} - 1)$
VL	0, si $N_V = 0$ N_V * S_V, sinon	N/A Déterminée par modèle

5.12 Relations entre zone d'influence (ZOI), granularité (G) et liste de valeurs (VL)

Les paramètres ZOI, PO et GL sont utilisés ensemble afin de garantir le comportement unique de l'outil (des outils) JPSEC appliqué(s), quel que soit l'ordre de progression du flux à codage JPEG 2000. En d'autres termes, la signature, les valeurs de code MAC et le flux codé par chiffrement que l'on obtient sont indépendants de l'ordre progressif du flux à codage JPEG 2000. La zone d'influence (ZOI) spécifie, dans son entièreté, la partie du flux à codage JPEG 2000 qui doit être protégée par l'outil JPSEC. L'ordre de traitement (PO), d'autre part, spécifie celui dans lequel l'outil JPSEC traite le flux codé. Le niveau de granularité (GL) spécifie les unités de protection contenant des séquences d'octets contiguës dans le flux codé réordonné. Finalement, chaque unité de protection correspond à une valeur contenue dans la liste de valeurs (VL), dans l'ordre où elle apparaît dans le flux codé réordonné. Cette relation peut être illustrée au moyen d'un seul exemple, où le flux à codage JPEG 2000 possède 1 pavé, 3 niveaux de résolution et 3 couches et où le nombre de composantes et de districts n'a pas d'importance. L'ordre progressif est RLCP dans le flux à codage JPEG 2000 original, la zone d'influence est représentée par les résolutions 0 et 1 et l'ordre de traitement (PO) est TRLCP. Les Figures 37 et 38 décrivent respectivement le réordonnancement du flux codé et le mappage à partir de chaque unité de protection vers la liste de valeurs (VL), quand le niveau de granularité (GL) est, selon le cas, une résolution ou une couche.

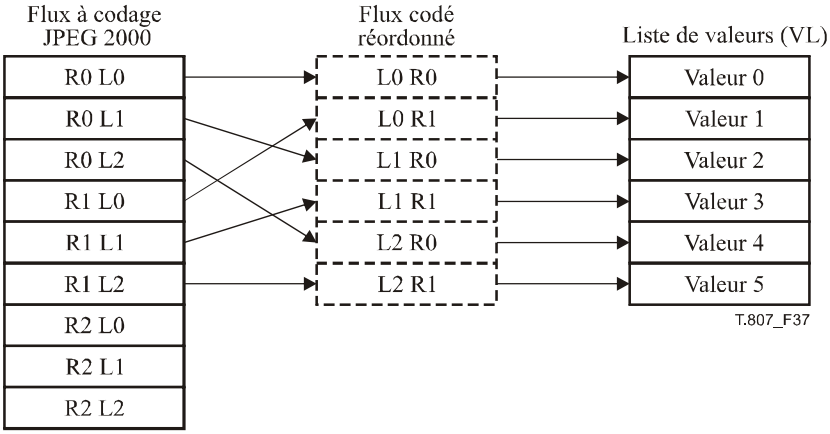


Figure 37 – Le niveau de granularité (GL) est une résolution

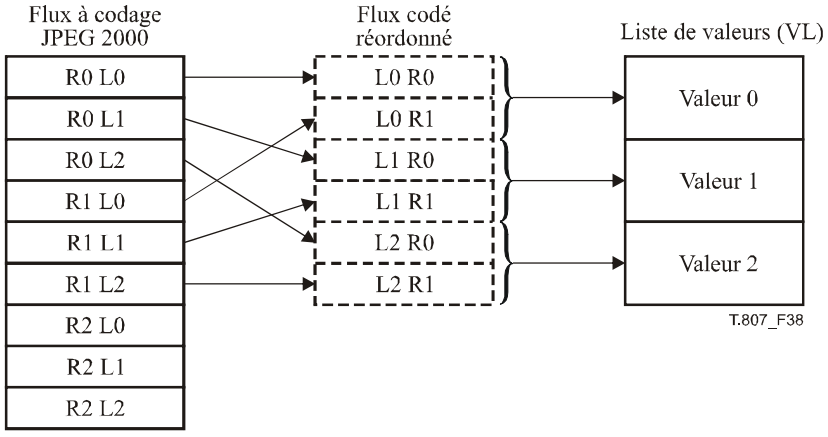


Figure 38 – Le niveau de granularité (GL) est une couche

NOTE – Le flux codé réordonné ne sert qu'à produire les valeurs contenues dans la liste de valeurs (VL). Le flux à codage JPSEC final aura le même ordre progressif que le flux à codage JPEG 2000 original.

5.13 Marqueur du flux codé entrant (INSEC)

Le marqueur du flux codé entrant (INSEC, *in-codestream security marker*) fournit un moyen supplémentaire de transmettre des informations de sécurité. Il est facultatif et est utilisé dans le cadre du marqueur SEC de sécurité. Spécifiquement, il est utilisé dans le cadre d'un outil JPSEC non normatif.

Plus précisément, le marqueur SEC est présent dans l'en-tête principal et donne des informations globales sur les outils JPSEC appliqués afin de protéger l'image. Le marqueur INSEC est présent dans les données du flux binaire proprement dites et fournit des paramètres supplémentaires ou secondaires pour l'outil JPSEC non normatif identifié par le

paramètre indiciel d'instance d'outil. L'indice d'instance d'outil contenu dans le marqueur INSEC doit donc correspondre à un des indices d'instance d'outil figurant dans l'en-tête principal.

Le segment marqueur INSEC peut être placé dans les données du flux binaire. Il utilise le fait que le décodeur arithmétique contenu dans le système JPEG 2000 arrête la lecture des octets du flux binaire quand il rencontre un marqueur de terminaison (c'est-à-dire deux octets avec une valeur supérieure à 0xFF8F).

Les informations transportées dans le segment marqueur INSEC sont applicables au ou aux blocs de code sécurisés précédents ou suivants jusqu'à ce qu'un autre marqueur INSEC soit trouvé.

Noter que l'inclusion de marqueurs INSEC produit un fichier qui peut ne pas être conforme à la Partie 1 de la norme JPEG 2000. Noter que certains décodeurs peuvent avoir de la difficulté à traiter un marqueur situé au milieu d'un paquet. L'insertion n'importe où à l'intérieur d'un paquet invalidera la longueur de paquet qui est indiquée dans l'en-tête de paquet. De même, il peut y avoir des problèmes avec le chiffrement et avec des marqueurs INSEC en raison:

a) d'un manque de restrictions d'émulation de marqueur dans le chiffrement;

b) d'une incapacité à localiser le marqueur proprement dit en présence d'un chiffrement.

La syntaxe du marqueur INSEC est définie dans la Figure 39.

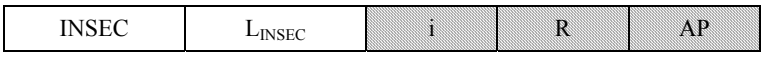


Figure 39 – Syntaxe de la sécurité du marqueur du flux codé entrant

INSEC: code de marqueur. Le Tableau 55 montre les longueurs et valeurs des symboles et paramètres pour le segment marqueur de flux codé entrant.

L_{INSEC}: longueur de segment marqueur en octets (non compris le marqueur). Noter que le segment marqueur INSEC devrait être verrouillé en octets.

i: indice d'instance d'outil correspondant à un des paramètres d'indice d'instance d'outil contenus dans le segment marqueur SEC et identifiant donc l'instance de l'outil JPSEC à laquelle ce marqueur INSEC se rapporte actuellement. Ce champ utilise la structure de segment RBAS.

R: zone d'applicabilité des informations de marqueur INSEC. Ce champ utilise la structure de segment FBAS.

AP: paramètres supplémentaires ou secondaires pour la méthode de protection. Le codeur devrait toujours vérifier qu'il n'émule pas de marqueur dans ce paramètre.

Tableau 55 – Valeurs paramétriques de sécurité du flux codé entrant (INSEC)

Paramètre	Longueur (bits)	Valeurs
INSEC	16	0xFF94
L_{INSEC}	16	2 ... $(2^{16} - 1)$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
R	Variable (FBAS)	Voir Tableau 56
AP	Variable	Définies par l'organisme d'enregistrement ou par l'application.

Tableau 56 – Valeurs de la zone d'applicabilité (R)

Numéro du bit de segment FBAS	Valeurs	Zone d'applicabilité
0	0	Blocs de code précédents
	1	Blocs de code suivants

Etant donné que le marqueur INSEC est utilisé dans le cadre d'outils JPSEC non normatifs, le format des paramètres supplémentaires ou secondaires est défini par l'outil proprement dit, qui est identifié par l'identificateur d'outil. Spécifiquement, les outils JPSEC non normatifs sont définis par un organisme d'enregistrement ou par des applications privées JPSEC. Donc, la définition de ces outils devrait comprendre l'usage du marqueur INSEC, s'il est autorisé.

6 Exemples d'utilisation de la syntaxe normative (paragraphe informatif)

6.1 Exemples de zone d'influence (ZOI)

Le présent paragraphe contient des exemples qui montrent comment la syntaxe de zone d'influence peut être utilisée.

Dans les exemples qui suivent, les indices supérieurs utilisés dans les paramètres Pzoi, Mzoi et Izoi correspondent à l'indice des items associés et non associés à l'image qui sont signalés par la structure de segment BAS dans le paramètre DCzoi, dans l'ordre où ils y apparaissent.

6.1.1 Exemple 1

Le présent paragraphe montre un exemple d'influence sur des niveaux de résolution supérieurs à 3 dans la région d'image dont le coin supérieur gauche est (100, 120) et dont le coin inférieur droit est (180, 210). Dans cet exemple, 9 octets sont nécessaires.

Tableau 57 – ZOI dans l'exemple 1

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à
$Zone^0$	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	101000_b	Régions d'image et niveaux de résolution spécifiés dans l'ordre
	$Pzoi^1$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	1_b	Izoi est décrit dans deux dimensions
		$Izoi^1$	8	$0110\ 0100_b$	Xul est 100
			8	$0111\ 1000_b$	Yul est 120
			8	$1011\ 0100_b$	Xlr est 180
			8	$1101\ 0010_b$	Ylr est 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Le complément des zones spécifiées est influencé par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	11_b	Mode maximal
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^3$	8	$0000\ 0010_b$	Des niveaux de résolution $\leq$ 2 sont spécifiés (c'est-à-dire que les niveaux de résolution > 3 sont spécifiés avec mode maximal et commutation sur le complément).

6.1.2 Exemple 2

Le présent paragraphe montre un exemple d'influence sur les blocs de code dont le coin supérieur gauche a un indice de 5 et le coin inférieur droit a un indice de 10 dans la sous-bande 1, au niveau de résolution 0. Dans cet exemple, 10 octets sont nécessaires.

Tableau 58 – ZOI dans l'exemple 2

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
Zone^0	DCzoi^1		1	1_b	Le segment verrouillé en octets suit
			1	0_b	Classe de description associée à l'image
			6	001000_b	Les niveaux de résolution spécifiés
	DCzoi^2		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	001100_b	Sous-bandes et blocs de code sont spécifiés
	Pzoi^3	Mzoi^3	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi^3	8	$0000\ 0000_b$	Indice du niveau de résolution égal à 0
	Pzoi^9	Mzoi^8	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi^8	8	$0000\ 0001_b$	La sous-bande 1 est spécifiée
	Pzoi^{10}	Mzoi^9	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi^9	8	$0000\ 0101_b$	L'indice de bloc de code pour le coin supérieur gauche est 5
			8	$0000\ 1010_b$	L'indice de bloc de code pour le coin inférieur droit est 10

6.1.3 Exemple 3

Le présent paragraphe montre un exemple d'influence sur les segments de données des octets 10 à 100 et des octets 10000 à 12000. Dans cet exemple, 12 octets sont nécessaires.

Tableau 59 – ZOI dans l'exemple 3

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
$Zone^0$	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010000_b	Etendues d'octet spécifiées après le marqueur SOD (début de données)
	$Pzoi^2$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	1_b	De multiples items sont spécifiés
			2	01_b	Mode d'étendue
			2	01_b	Izoi utilise 16 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Nzoi^2$	8	$0000\ 0010_b$	Nombre de segments de données égal à 2
		$Izoi^{21}$	16	$0000\ 0000_b$ $0000\ 1010_b$	L'emplacement de l'octet de début est le 10^e (octets).
			16	$0000\ 0000_b$ $0110\ 0100_b$	L'emplacement de l'octet de fin est le 100^e (octets).
		$Izoi^{21}$	16	$0010\ 0111_b$ $0001\ 0000_b$	L'emplacement de l'octet de début est le 10000^e (octets).
			16	$0010\ 1110_b$ $1110\ 0000_b$	L'emplacement de l'octet de fin est le 12000^e (octets).

6.1.4 Exemple 4

Le présent paragraphe montre un exemple d'influence sur le niveau de résolution 0, dans lequel le segment de l'octet 10 à 100 correspond aux données du niveau de résolution 0. Dans cet exemple, 10 octets sont nécessaires.

Tableau 60 – ZOI dans l'exemple 4

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
$Zone^0$	$DCzoi^1$		1	1_b	Le segment verrouillé en octets suit
			1	0_b	Classe de description associée à l'image
			6	001000_b	Niveaux de résolution spécifiés dans l'ordre
	$DCzoi^2$		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010000_b	Etendues d'octet spécifiées
	$Pzoi^1$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^1$	8	$0000\ 0000_b$	Niveau de résolution: 0.

Tableau 60 – ZOI dans l'exemple 4

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
$Zone^0$	$Pzoi^2$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Des items isolés sont spécifiés
			2	01_b	Mode d'étendue
			2	01_b	Izoi utilise 16 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^1$	16	0000 0000 $0000\ 1010_b$	L'emplacement de l'octet de début est le 10^e (octets).
			16	0000 0000 $0110\ 0100_b$	L'emplacement de l'octet de fin est le 100^e (octets).

6.1.5 Exemple 5

Le présent paragraphe montre un exemple d'influence sur les niveaux de résolution supérieurs à 3 dans les pavés dont l'indice supérieur gauche est 0 et dont l'indice inférieur droit est 5, ainsi que sur les couches inférieures ou égales à 5 dans les pavés dont l'indice supérieur gauche est 10 et dont l'indice de pavé inférieur droit est 15. Dans cet exemple, 13 octets sont nécessaires.

Tableau 61 – ZOI dans l'exemple 5

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	2	Le nombre de zones est deux
$Zone^0$	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	$01\ 1000_b$	Pavés et niveaux de résolution spécifiés dans l'ordre
	$Pzoi^2$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^2$	8	$0000\ 0000_b$	L'indice de pavé supérieur gauche est 0
			8	$0000\ 0101_b$	L'indice de pavé inférieur droit est 5
	$Pzoi^3$	$Mzoi^3$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Le complément des zones spécifiées est influencé par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	11_b	Mode maximal
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^3$	8	$0000\ 0010_b$	Les niveaux de résolution ≤ 2 sont spécifiés. (C'est-à-dire que les niveaux de résolution > 3 sont spécifiés avec mode maximal et commutation sur le complément.)

Tableau 61 – ZOI dans l'exemple 5

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
Zone[1]	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	010100_b	Pavés et couches sont spécifiés dans l'ordre
	Pzoi[2]	Mzoi[2]	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi[2]	8	$0000\ 1010_b$	L'indice de pavé supérieur gauche est 10
			8	$0000\ 1111_b$	L'indice de pavé inférieur droit est 15
	Pzoi[4]	Mzoi[4]	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	11_b	Mode maximal
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi[4]	8	$0000\ 0101_b$	Les couches $\leq$ 5 sont spécifiées avec mode maximal

6.1.6 Exemple 6

Le présent paragraphe montre un exemple d'influence sur le segment d'en-tête de l'octet 10 à l'octet 100. Dans cet exemple, 8 octets sont nécessaires.

Tableau 62 – ZOI dans l'exemple 6

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
Zone[0]	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	001000_b	Des étendues d'octet après le marqueur SEC sont spécifiées
	Pzoi[3]	Mzoi[3]	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	01_b	Mode d'étendue
			2	01_b	Izoi utilise 16 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		Izoi[3]	16	$0000\ 0000$ $0000\ 1010_b$	L'emplacement de l'octet de début est le 10^e (octets)
			16	$0000\ 0000$ $0110\ 0100_b$	L'emplacement de l'octet de fin est le 100^e (octets)

6.2 Exemples de modèle d'informations sur les clés

6.2.1 Exemple 1

Le Tableau 63 montre l'exemple d'une clé unique secrète (128 bits) qui sert à déchiffrer un flux codé. Cette clé est identifiée au moyen d'un identificateur URI et extraite du serveur distant de clés fondées sur un identificateur URI, au cours de l'étape de déchiffrement.

Tableau 63 – Informations sur les clés dans l'exemple 1

Paramètre		Longueur (bits)	Valeur	Signification déduite
LK_{KT}		16	128	Longueur de clé: 128 bits
KID_{KT}		8	2	L'identificateur URI de clé secrète est identifié
G_{KT}	PO	16	000 001 010 011 100 0_b	Ordre de traitement: pavé-résolution-couche-composante-district
	GL	8	0000 1001_b	L'unité de protection est l'aire totale identifiée dans la zone ZOI
V_{KT}	N_V	16 (RBAS)	1	Le nombre de valeurs contenues dans la liste de valeurs V est 1
	S_V	8 (RBAS)	19	La longueur des informations sur les clés est de 19 octets
	V1	152	https://serveur/fichier	La clé secrète peut être extraite à partir du lien https://serveur/fichier.

6.2.2 Exemple 2

Le Tableau 64 montre que l'exemple d'un certificat X.509 sert à authentifier un flux codé, où le certificat X.509 a été imbriqué dans le paramètre KI_{KT} par la méthode de codage DER.

Tableau 64 – Informations sur les clés dans l'exemple 2

Paramètre			Longueur (bits)	Valeur	Signification déduite
LK_{KT}			16	1024	Longueur de clé: 1024 bits
KID_{KT}			8	2	Le certificat X.509 est identifié
G_{KT}	PO		16	000 001 010 011 100 0_b	Ordre de traitement: pavé-résolution-couche-composante-district
	GL		8	0000 1001_b	L'unité de protection est l'aire totale identifiée dans la zone ZOI
V_{KT}	N_V		16 (RBAS)	1	Le nombre de valeurs contenues dans la liste de valeurs V est 1
	S_V		8 (RBAS)	Variable	Longueur du certificat X.509
	V1	ER_{KT}	8	1	Certificat X.509 codé par la méthode de codage DER
		$LCER_{KT}$	16	Variable	Longueur du paramètre CER_{KT}
		CER_{KT}	Variable	Valeur du certificat	Le certificat avec clé publique de 1024 bits a été imbriqué

6.2.3 Exemple 3

Le Tableau 65 montre une unique clé publique, servant à authentifier un flux codé, qui a été imbriquée dans le paramètre KI_{KT}.

Tableau 65 – Informations sur les clés dans l'exemple 3

Paramètre		Longueur (bits)	Valeur	Signification déduite
LK_{KT}		16	1024	Longueur de clé: 1024 bits
KID_{KT}		8	1	La clé publique est identifiée
G_{KT}	PO	16	000 001 010 011 100 0_b	Ordre de traitement: pavé-résolution-couche-composante-district
	GL	8	0000 1001_b	L'unité de protection est l'aire totale identifiée dans la zone ZOI
V_{KT}	N_V	16 (RBAS)	1	Le nombre de valeurs contenues dans la liste de valeurs V est 1
	S_V	8 (RBAS)	256	La longueur de clé publique est 256 octets
	V1	2048	Valeur de clé publique	La clé publique a été imbriquée

6.2.4 Exemple 4

Le Tableau 66 montre que de clés multiples secrètes servent à déchiffrer un flux codé, où différentes clés secrètes sont utilisées pour différentes couches.

Tableau 66 – Informations sur les clés dans l'exemple 4

Paramètre		Longueur (bits)	Valeur	Signification déduite
LK_{KT}		16	128	Longueur de clé: 128 bits
KID_{KT}		8	3	URI pour clé secrète identifié
G_{KT}	PO	16	000 001 010 011 1000_b	Ordre de traitement: pavé-résolution-couche-composante-district
	GL	8	0000 0100_b	L'unité de protection est la couche
V_{KT}	N_V	16 (RBAS)	3	Le nombre de valeurs contenues dans la liste de valeurs V est 3
	S_V	8 (RBAS)	16	La longueur de chaque Vn est 16 octets
	V1	128	https://serveur/1	La clé secrète pour la 1re couche peut être extraite à partir de https://serveur/1.
	V2	128	https://serveur/2	La clé secrète pour la 2e couche peut être extraite à partir de https://serveur/2.
	V3	128	https://serveur/3	La clé secrète pour la 3e couche peut être extraite à partir de https://serveur/3.
	V4	128	https://serveur/4	La clé secrète pour la 4e couche peut être extraite à partir de https://serveur/4.

6.3 Exemples d'outil JPSEC normatif

Les exemples suivants décrivent comment la zone ZOI et les modèles de clé peuvent servir à exécuter des services de sécurité de base tels que le chiffrement et l'authentification sur une image JPEG 2000.

6.3.1 Exemple 1

Une image est codée selon la norme JPEG 2000 et a trois résolutions. Dans cet exemple, la première résolution n'est pas chiffrée afin d'offrir une capacité de prévisualisation; la seconde et la troisième résolutions sont chiffrées respectivement avec les clés k1 et k2. L'image d'entrée est, dans ce cas, codée dans l'ordre de progression RLCP et possède: 1 pavé, 3 résolutions, 3 couches, Nc composantes et Np districts (le nombre de composantes et de districts n'est pas significatif dans cet exemple spécifique). Le chiffrement est effectué au moyen de l'algorithme AES en mode de chaînage CBC sans bourrage (par extraction cryptographique), au moyen de la clé k0 afin de chiffrer la résolution 1 et au moyen de la clé k2 afin de chiffrer la résolution 2, la résolution 0 étant laissée non chiffrée.

L'outil JPSEC signale comment un consommateur JPSEC devrait déchiffrer le flux à codage JPSEC. Tout d'abord, l'identificateur d'outil du modèle de déchiffrement est signalé. Deux zones ZOI sont spécifiées pour la résolution 1 et pour son étendue d'octet correspondante B0-B1, ainsi que pour la résolution 2 et son étendue d'octet correspondante B2-B3. Les paramètres du modèle de déchiffrement déterminent que le chiffrement AES est appliqué sans bourrage (par extraction cryptographique). Les informations concernant le calcul de clé et le fait que différentes clés soient appliquées à différentes résolutions sont signalées avec les paramètres d'informations sur les clés. Spécifiquement, la granularité de

clé est spécifiée en tant que résolution, de sorte que chaque résolution possède une clé différente, où l'ordre de traitement est signalé comme étant: TRLCP. Les informations sur les clés pour chaque résolution sont contenues dans la liste de valeurs de clés. Le chiffrement est effectué sur le flux codé en chiffrant à la fois les en-têtes de paquet et les corps de paquet. La granularité de chiffrement est la résolution, où le traitement est effectué dans l'ordre TRLCP qui est le même que celui du flux codé original. Comme les deux résolutions sont chiffrées séparément, deux vecteurs d'initialisation (IV) sont requis et sont contenus dans la liste de valeurs.

Noter que les résultats d'un cryptogramme de paquet sont spécifiés par l'ordre de traitement et sont donc indépendant de l'ordre de progression du flux codé d'entrée. Cependant, l'emplacement des paquets chiffrés dans le flux codé de sortie suit l'ordre des paquets du flux codé d'entrée.

Tableau 67 – Segment marqueur SEC pour l'exemple 1

Paramètre			Longueur (bits)	Valeurs	Signification
SEC			16	0xFF65	Marqueur SEC
L_{SEC}			16 (RBAS)	0x82	Longueur de segment marqueur SEC: 130 octets
Z_{SEC}			8 (RBAS)	0	Indice de ce segment marqueur SEC
P_{SEC}	F_{PSEC}		1	0_b	La structure de segment FBAS ne suit pas
		F_{INSEC}	1	0_b	INSEC n'est pas utilisé
		$F_{multiSEC}$	1	0_b	Un seul segment marqueur SEC est utilisé
		F_{mod}	2	00_b	Des données originales JPEG 2000 ont été modifiées
		F_{TRLCP}	1	0_b	L'usage de balise indicielle TRLCP n'est pas défini dans P_{SEC}
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	Nombre d'outils de sécurité égal à 1
	I_{max}		8 (RBAS)	0000000_b	Indice maximal d'instance d'outil égal à 0
t			8 (FBAS)	0	Outil JPSEC normatif
i			8 (RBAS)	0	Indice d'instance d'outil
ID_T			8	1	Modèle de déchiffrement
L_{zoi}			16 (RBAS)	0x17	Longueur de zone ZOI égale à 23 octets
ZOI			184	Voir Tableau 68	Zone d'influence pour cet outil
L_{PID}			16 (RBAS)	0x5e	Longueur de P_{ID} égale à 94 octets
P_{ID}			752	Voir Tableau 69	Paramètres pour cette technologie

Tableau 68 – Exemple de zone ZOI

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	2	Nombre de zones égal à 1
$Zone^0$	DC_{ZOI}^1		1	1_b	Le segment verrouillé en octets suit
			1	0_b	Classe de description associée à l'image
			6	001000_b	La résolution est spécifiée
	DCzoi[2]		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010000_b	Des étendues d'octet après le marqueur SOD (début de données) sont spécifiées
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		I_{ZOI}	8	$0000\ 0001_b$	La résolution 1 est spécifiée
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	01_b	Mode d'étendue
			2	01_b	Izoi utilise des entiers de 16 bits
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^{21}$	16	0x31CC	L'emplacement de l'octet de début est le 12748^e (octets). (B0)
			16	0xA3E8	L'emplacement de l'octet de fin est le 41960^e (octets). (B1)
$Zone^1$	DC_{ZOI}^1		1	1_b	Le segment verrouillé en octets suit
			1	0_b	Classe de description associée à l'image
			6	001000_b	La résolution est spécifiée
	DCzoi[2]		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010000_b	Des étendues d'octet après le marqueur SOD (début de données) sont spécifiées
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		I_{ZOI}^1	8	$0000\ 0010_b$	La résolution 2 est spécifiée
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_{b2}	Un item unique est spécifié
			2	01_b	Mode d'étendue
			2	10_b	Izoi utilise 32 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^2$	32	0xA3EE	L'emplacement de l'octet de début est le 41966^e (octets). (B2)
			32	0x21101	L'emplacement de l'octet de fin est le 135425^e (octets). (B3)

Tableau 69 – Exemple de P_{ID}

Paramètre		Longueur (bits)	Valeurs	Signification
T_{ID}		432	Voir Tableau 70	Modèles de déchiffrement
PD		8 (FBAS)	0_b	Le segment verrouillé en octets ne suit pas.
			0_b	Le domaine des pixels n'est pas utilisé
			0_b	Le domaine des coefficients d'ondelette n'est pas utilisé
			0_b	Le domaine des coefficients d'ondelette quantifiés n'est pas utilisé
			1_b	Le domaine du flux codé est utilisé
			000_b	Réservé pour utilisation par l'ISO
F_{PD}		8 (FBAS)	0_b	L'octet de segment FBAS ne suit pas
			1_b	Seul le corps de paquet est chiffré
			000000_b	Réservé pour utilisation par l'ISO
G	PO	16	000 001 010 011 100 0_b	Ordre de traitement: pavé-résolution-couche-composante-district.
	GL	8	0000 0011_b	L'unité de protection est le niveau de résolution
V	N_V	16 (RBAS)	2	Le nombre de valeurs contenues dans la liste de valeurs V est 2
	S_V	8 (RBAS)	16	La longueur de chaque Vn est 16 octets.
	V1	128	IV0	Valeur du vecteur d'initialisation pour R1
	V2	128	IV1	Valeur du vecteur d'initialisation pour R2

Tableau 70 – Exemple de modèle de déchiffrement

Paramètre		Longueur	Valeur (dans l'ordre)	Signification déduite
ME_{decry}		8	0	Une émulation de marqueur s'est produite
CT_{decry}		16	0001_b	Chiffrement par blocs (AES)
CP_{decry}	M_{bc}	6	100000_b	Mode CBC. Bits non justifiés par bourrage
	P_{bc}	2	00_b	Extraction cryptographique
	SIZ_{bc}	8	16	Longueur de bloc (16 octets, 128 bits)
	KT_{bc}	392	Voir Tableau 71	Modèle de clé

Tableau 71 – Exemple de modèle de clé

Paramètre		Longueur (bits)	Valeur	Signification déduite
LK_{KT}		16	128	Longueur de clé: 128 bits
KID_{KT}		8	2	URI pour clé secrète
G_{KT}	PO	16	0 000 001 010 011 100_b	Ordre de traitement: pavé-résolution-couche-composante-district.
	GL	8	0000 0011_b	L'unité de protection est le niveau de résolution
V_{KT}	N_V	32 (RBAS)	2	Le nombre de valeurs contenues dans la liste de valeurs V est 2
	S_V	8 (RBAS)	19	Longueur de chaque Vn: 19 octets
	V1	152	https://serveur/key1	La clé secrète pour le niveau de résolution 1 peut être extraite à partir de https://serveur/key1.
	V2	152	https://serveur/key2	La clé secrète pour le niveau de résolution 2 peut être extraite à partir de https://serveur/key2.

6.3.2 Exemple 2

Dans ce cas, l'authentification est appliquée à la même image JPEG 2000 que ci-dessus. Dans cet exemple, les trois résolutions et les trois couches par résolution sont authentifiées, où l'authentification de chaque résolution utilise une clé différente. Comme il y a trois résolutions, il y a trois clés et comme il y a trois couches par résolution, il y aura trois valeurs de code MAC par résolution. Il y aura donc un total de neuf valeurs de code MAC pour la totalité de l'image JPSEC. Spécifiquement,

- la résolution 0 possède les valeurs de code MAC M0, M1, M2 (une pour chaque couche) au moyen de key0;
- la résolution 1 possède les valeurs de code MAC M3, M4, M5 (une pour chaque couche) au moyen de key1;
- la résolution 2 possède les valeurs de code MAC M6, M7, M8 (une pour chaque couche) au moyen de key2.

Cet exemple décrit comment l'authentification peut être signalée ainsi que la flexibilité fournie par la zone ZOI et par les outils de granularité. Comme dans l'exemple précédent, l'image d'entrée est codée dans l'ordre de progression RLCP et contient 1 pavé, 3 résolutions, 3 couches, Nc composantes et Np districts (le nombre de composantes et de districts n'est pas important dans cet exemple spécifique). L'authentification est effectuée au moyen du code HMAC avec l'algorithme SHA-1.

L'outil JPSEC signale comment un consommateur JPSEC peut vérifier ou authentifier le contenu JPSEC protégé. Tout d'abord, l'identificateur d'outil du modèle d'authentification est signalé. Puis la zone ZOI sert à signaler qu'il y a trois résolutions avec les étendues d'octet associées à chaque résolution. Les paramètres du modèle d'authentification signalent que le code HMAC est appliqué au moyen de l'algorithme SHA-1. Le modèle d'informations de clé fournit les informations sur les clés y compris l'indication que la granularité de clé est la résolution, avec les informations pour chacune des trois clés, contenues dans la liste de valeurs pour les clés. Le domaine de traitement pour authentification est spécifié comme étant le flux codé y compris les en-têtes de paquet. La granularité d'outil pour l'authentification est spécifiée comme étant la couche: il y a donc trois codes MAC pour chaque résolution, sur un total de neuf valeurs de code MAC. La liste de valeurs contient les neuf valeurs de code MAC. L'ordre de traitement pour l'opération précédente a été identifié comme étant TRLCP, c'est-à-dire l'ordre original du flux codé.

Noter que l'utilisation de l'ordre de traitement dans le champ de granularité garantit que les mêmes valeurs de code MAC seront obtenues, quel que soit l'ordre de progression du flux codé.

Noter que, alors que cet exemple a démontré l'utilisation des codes MAC, la même méthode peut servir à signaler l'utilisation de multiples signatures numériques.

Tableau 72 – Le segment marqueur SEC

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
SEC			16	0xFF65	Marqueur SEC
L_{SEC}			16	0x0099	Longueur de segment marqueur SEC
Z_{SEC}			8 (RBAS)	0	Indice de ce segment marqueur SEC
P_{SEC}	F_{PSEC}		1	0_b	La structure de segment FBAS ne suit pas
		F_{INSEC}	1	0_b	Le segment marqueur INSEC n'est pas utilisé
		$F_{multiSEC}$	1	0_b	Il n'y a qu'un seul segment marqueur SEC dans ce flux codé
		F_{mod}	1	0_b	Les données originales JPEG 2000 n'ont pas été modifiées
		F_{TRLCP}	1	0_b	La balise indicielle TRLCP n'est pas utilisée
		Padding	3	000_b	La balise indicielle TRLCP n'est pas utilisée
	N_{tools}		7	1	Un seul outil est utilisé dans ce flux codé
	I_{max}		7	0	L'indice maximal d'instance d'outil est 0
$Tool^0$	t		8 (FBAS)	0	Outil JPSEC normatif
	i		8 (RBAS)	0	Indice d'instance d'outil
	ID_T		8	2	Cet outil normatif utilise un modèle d'authentification
	L_{ZOI}		16 (RBAS)	0x20	Longueur de zone ZOI: 32 octets
	ZOI		256	Tableau 73	Zone couverte de l'image
	L_{PID}		16 (RBAS)	0x6c	Longueur de $P_{ID:}$ 108 octets
	P_{ID}		928	Tableau 74	Paramètres pour outil JPSEC

Tableau 73 – Signalisation de zone ZOI

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Le nombre de zones est 1
$Zone^0$	DC_{zoi}^1		1	1_b	Le segment verrouillé en octets suit
			1	0_b	Classe de description associée à l'image
			6	001000_b	Niveaux de résolution spécifiés dans l'ordre
	DC_{zoi}^2		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010000_b	Etendues d'octets spécifiées
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	01_b	Mode d'étendue
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^1$	8	0	Le début de l'étendue est 0
			8	2	La fin de l'étendue est 2
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	1_b	Multiples items spécifiés
			2	01_b	Mode d'étendue
			2	10_b	Izoi utilise des entiers de 32 bits
			1	0_b	Izoi est décrit dans une seule dimension
		N_{ZOI}	8 (RBAS)	3	Nombre de I_{ZOI} 3
		$Izoi^1$	32	104	L'emplacement de l'octet de début est le 104^e (octets).
			32	12762	L'emplacement de l'octet de fin est le 12762^e (octets).
		I_{ZOI}^2	32	12768	L'emplacement de l'octet de début est le 12768^e (octets).
			32	41980	L'emplacement de l'octet de fin est le 41980^e (octets).
		I_{ZOI}^3	32	41986	L'emplacement de l'octet de début est le 41986^e (octets).
			32	135445	L'emplacement de l'octet de fin est le 135445^e (octets).

Tableau 74 – Paramètres de signalisation d'identificateur P_{ID}

Paramètre					Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
T_{auth}	M_{auth}				8	0	Méthode d'authentification: hachage.
	P_{auth}	M_{HMAC}			8	1	Un code HMAC est utilisé pour l'authentification
		H_{HMAC}			8	1	L'algorithme SHA-1 est utilisé pour le hachage
		KT_{HMAC}	LK_{KT}		16	128	Longueur de la clé en bits
			KID_{KT}		8	3	KI_{KT} contient l'identificateur URI de la clé privée
			G_{KT}	PO	16	0000001010011100_b	L'ordre est: pavé-résolution-couche-composante-district
				GL	8	00000011_b	La granularité des clés est la résolution
			V_{KT}	N_V	16 (RBAS)	3	Il y a 3 clés dans la liste
				S_V	8 (RBAS)	8	Longueur de chaque clé: 8 octets
				VL	64	Key0	La première clé est *key*0, pour la résolution 0.
					64	Key1	La deuxième clé est *key*1, pour la résolution 1.
					64	Key2	La troisième clé est *key*2, pour la résolution 2.
		SIZ_{HMAC}			16	20	Longueur du code MAC 20
PD					8 (FBAS)	0_b	Le segment verrouillé en octets ne suit pas
						0_b	Le domaine des pixels n'est pas utilisé
						0_b	Le domaine des coefficients d'ondelette n'est pas utilisé
						0_b	Le domaine des coefficients d'ondelette quantifiés n'est pas utilisé
						1_b	Le domaine du flux codé est utilisé
						000_b	Réservé pour utilisation par l'ISO
F_{PD}					8 (FBAS)	0_b	L'octet de segment FBAS ne suit pas
						0_b	Aussi bien l'en-tête que le corps du paquet est chiffré
						000000_b	Réservé pour utilisation par l'ISO
G	PO				16	0000010100111000_b	L'ordre est: pavé-résolution-couche-composante-district
	GL				8	00000100_b	La granularité d'outil est la couche
V	N_V				32 (RBAS)	9	Il y a 9 codes MAC (3 par résolution)
	S_V				8 (RBAS)	20	Longueur de chaque code MAC 20 octets
	VL				160	*M*0	Le premier code MAC est *M*0
					160	*M*1	Le second code MAC est *M*1
					160	*M*2	Le troisième code MAC est *M*2
					160	*M*3	Le quatrième code MAC est *M*3
					160	*M*4	Le cinquième code MAC est *M*4
					160	*M*5	Le sixième code MAC est *M*5
					160	*M*6	Le septième code MAC est *M*6
					160	*M*7	Le huitième code MAC est *M*7
					160	*M*8	Le neuvième code MAC est *M*8

6.4 Exemples de champ de distorsion

Le présent paragraphe fournit quelques exemples simples sur l'utilisation du champ de distorsion.

6.4.1 Exemple 1

Cet exemple se fonde sur celui de l'exemple 3 de zone ZOI dans le § 6.1.3 afin de montrer comment des valeurs de distorsion peuvent être associées aux deux segments de données signalés par la zone ZOI dans cet exemple. Pour mémoire, l'exemple 3 du § 6.1.3 signalait deux segments de données: (1) les octets 10 à 100 et (2) les octets 10000 à 12000. De façon à associer des champs de distorsion à ces deux segments de données, il faut deux étapes. Tout d'abord, le champ de distorsion est signalé dans DCzoi. En second lieu, les valeurs de distorsion sont signalées au moyen de $Pzoi^2$. Les seuls changements par rapport à l'exemple 3 de zone ZOI dans le § 6.1.3 consistent donc à régler le bit de champ de distorsion dans DCzoi et à ajouter $Pzoi^2$ (les neuf dernières lignes du Tableau 75).

Tableau 75 – Association du champ de distorsion à deux segments de données (extension de l'exemple 3 de zone ZOI au § 6.1.3)

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
$Zone^0$	DCzoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	010001_b	Des étendues d'octet après le marqueur SOD (début de données) sont spécifiées et des champs de distorsion associés sont spécifiés
	$Pzoi^2$	$Mzoi^2$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	1_b	De multiples items sont spécifiés
			2	01_b	Mode d'étendue
			2	01_b	Izoi utilise 16 bit pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Nzoi^2$	8 (RBAS)	2	Nombre de segments de données: 2.
		$Izoi^{2,1}$	16	0000 0000 0000 1010_b	L'emplacement de l'octet de début est le 10^e (octets).
			16	0000 0000 0110 0100_b	L'emplacement de l'octet de fin est le 100^e (octets).
		$Izoi^{2,2}$	16	0010 0111 0001 0000_b	L'emplacement de l'octet de début est le 10000^e (octets).
			16	0010 1110 1110 0000_b	L'emplacement de l'octet de fin est le 12000^e (octets).
	$Pzoi^6$	$Mzoi^6$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	1_b	De multiples items sont spécifiés
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits servant à représenter chaque valeur de distorsion
			1	0_b	Izoi est décrit dans une seule dimension
		$Nzoi^6$	8 (RBAS)	2	Nombre de segments de données: 2.
		$Izoi^{6,1}$	8	Valeur D1	Valeur de distorsion pour le premier segment
		$Izoi^{6,2}$	8	Valeur D2	Valeur de distorsion pour le second segment

6.4.2 Exemple 2

Cet exemple décrit comment des valeurs de distorsion peuvent être associées à des paquets JPEG 2000. Le champ DCzoi spécifie une étendue de 4 paquets et le champ de distorsion est également signalé. Le champ $Pzoi^1$ donne l'étendue des paquets et $Pzoi^2$ décrit la distorsion associée à chacun de ces paquets. Noter que, comme $Pzoi^1$ spécifie une étendue de longueur 4 et que $Pzoi^2$ spécifie 4 valeurs, chaque item contenu dans l'étendue est associé à 1 valeur, p. ex. chaque paquet est associé à 1 distorsion.

Tableau 76 – Signalisation d'une étendue de paquets et association de distorsions à chaque paquet

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8 (RBAS)	1	Nombre de zones égal à 1
$Zone^0$	DCzoi		1	0	Le segment verrouillé en octets ne suit pas
			1	1_b	Classe de description non associée à l'image
			6	100001_b	Paquets spécifiés et champs de distorsion associés spécifiés
	$Pzoi^1$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	0_b	Un item unique est spécifié
			2	01_b	Mode d'étendue
			2	00_b	Izoi utilise des entiers de 8 bits
			1	0_b	Izoi est décrit dans une seule dimension
		$Nzoi^1$	8 (RBAS)	1	Nombre de segments de données: 1.
		$Izoi^{11}$	8	$0000\ 0000_b$	Le paquet de début est le numéro 0.
			8	$0000\ 0011_b$	Le paquet de fin est le numéro 3.
	$Pzoi^6$	$Mzoi^6$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par l'outil JPSEC
			1	1_b	De multiples items sont spécifiés
			2	10_b	Mode indiciel
			2	00_b	Izoi utilise 8 bits servant à représenter chaque valeur de distorsion
			1	0_b	Izoi est décrit dans une seule dimension
		$Nzoi^6$	8 (RBAS)	4	Nombre de segments de données: 4.
		$Izoi^{6,1}$	8	Valeur D1	Valeur de distorsion pour le premier paquet
		$Izoi^{6,2}$	8	Valeur D2	Valeur de distorsion pour le second paquet
		$Izoi^{6,3}$	8	Valeur D3	Valeur de distorsion pour le troisième paquet
		$Izoi^{6,4}$	8	Valeur D4	Valeur de distorsion pour le quatrième paquet

7 Organisme d'enregistrement JPSEC

7.1 Introduction générale

Le mécanisme d'enregistrement JPSEC garantit l'identification univoque des outils de sécurité non normatifs qui suivent la norme JPSEC et qui pourront encore être proposés ou développés comme outils JPSEC non normatifs, s'ajoutant à ceux qui sont énumérés dans l'Annexe B. Cet enregistrement est effectué par un organisme d'enregistrement JPSEC. Il doit être conforme aux directives du comité JTC 1. L'enregistrement de ces nouveaux outils JPSEC est contrôlé par le processus défini dans le présent paragraphe.

Les demandeurs peuvent soumettre les technologies qu'ils voudraient faire inclure dans la liste de référence JPSEC. Noter que l'usage de l'outil JPSEC est spécifié par un marqueur JPSEC présent dans le flux codé. Quand une application trouve un identificateur JPSEC inconnu, elle peut consulter un organisme d'enregistrement JPSEC et obtenir les informations enregistrées sur l'outil.

7.2 Critères d'admissibilité des demandeurs d'enregistrement

Les demandeurs admissibles doivent être des organisations homologuées par leur Organisme national.

7.3 Dépôt des demandes d'enregistrement

Les demandes d'enregistrement de nouveaux outils JPSEC doivent être publiées par un organisme d'enregistrement JPSEC sur un site IP.

Le site IP doit contenir les formulaires de demande d'enregistrement, de demande de mise à jour, de notification d'attribution ou de mise à jour et de rejet de candidature.

Tous les formulaires doivent inclure:

- le nom de l'organisation requérante;
- l'adresse de l'organisation requérante;
- le nom, le titre, l'adresse postale/électronique, le numéro de téléphone/télécopie d'une personne de contact dans l'organisation.

Les formulaires de demande d'enregistrement et de demande de mise à jour doivent également comprendre les entrées suivantes:

- nom de l'outil JPSEC (obligatoire);
- type d'outil JPSEC, p. ex. signature numérique, filigranage, chiffrement, brassage, production et gestion des clés, authentification (facultatif);
- descriptif technique abrégé (obligatoire);
- descriptif général de l'outil (obligatoire);
- description d'un cas de figure opérationnel à titre d'exemple (facultatif);
- spécification de la syntaxe des paramètres, y compris les valeurs possibles (facultatif);
- directives d'usage optimal (facultatif);
- état des droits IPR, p. ex. propriétaire, ayant droit (facultatif);
- droits IPR nécessaires à l'utilisation (obligatoire);
- restrictions d'utilisation, p. ex. conditions d'exportation (facultatif);
- renseignements relatifs aux importations par téléchargement d'implémentations (facultatif);
- remarques additionnelles, motifs, références… (facultatif);
- exigences relatives à la confidentialité d'entrées sélectionnées (facultatif);
- durée requise de l'enregistrement d'outil (facultatif).

L'organisme d'enregistrement JPSEC doit également offrir des matériaux didactiques afin d'aider les demandeurs à préparer leur demande.

7.4 Examen et suivi des demandes

Le présent paragraphe définit le processus permettant à l'organisme d'enregistrement JPSEC d'apporter une révision et une réponse à des applications afin de garantir l'impartialité de traitement.

Un comité de révision technique est activé afin de passer en revue les demandes. Ce comité se compose des membres de l'ISO/CEI JTC 1/SC 29/GT 1 et de l'organisme d'enregistrement JPSEC. Le comité de révision examine les demandes lors d'une réunion du GT 1 dans les neuf mois qui suivent leur soumission.

Le comité de révision accepte ou rejette la demande sur la base des critères de rejet indiqués dans le § 7.5.

Si accepté, le nouvel outil JPSEC se fait attribuer un identificateur (ID) pour une période spécifiée. La syntaxe d'identification doit être conforme au § 5.6.3. Le comité de révision approuve les informations de description d'outil JPSEC énumérées dans le § 7.3. Cet identificateur doit ensuite être utilisé pour la signalisation dans le flux à codage JPSEC.

Une fois que la demande a été révisée et acceptée, l'organisme d'enregistrement JPSEC envoie au demandeur une réponse favorable ou défavorable à sa requête d'enregistrement. La réponse notifiée au demandeur doit inclure une brève explication des résultats de la révision technique et doit être renvoyée au demandeur dans les neuf mois qui suivent la date de dépôt de la demande.

Une réponse défavorable peut faire l'objet d'un recours en appel si le requérant d'enregistrement estime qu'il y a eu une erreur dans le rejet, ou quand un complément d'information est requis afin de clarifier des problèmes ou des interrogations. Si le requérant d'enregistrement requiert un examen complémentaire allant au-delà du processus de l'organisme, il peut soumettre son cas pour examen par le plus large GT 1 lors de la prochaine réunion appropriée de celui-ci. Il pourra alors être tenu d'offrir des informations complémentaires à la demande des experts qui, sous l'autorité du GT 1, donneront finalement une réponse définitive d'acceptation ou de rejet. Afin qu'une demande rejetée soit révisée par le GT 1, le requérant d'enregistrement doit resoumettre sa proposition par l'entremise de son Organisme national, en spécifiant la raison pour laquelle la soumission nécessite un examen par le GT 1.

7.5 Rejet de demandes

Les critères de rejet d'une demande sont les suivants:

- le demandeur n'est pas admissible;
- les honoraires appropriés ne sont pas payés (le cas échéant);
- il existe déjà un item homologué et enregistré, dont le contenu est identique à la soumission;
- les informations contenues dans la demande sont incomplètes ou incompréhensibles;
- la justification de l'inclusion dans le registre n'est pas adéquate. L'outil JPSEC candidat devrait démontrer qu'il apporte un service de sécurité utile et devrait donner des exemples de cas de figure le cas échéant;
- l'autorité considère qu'il n'y a pas assez d'originalité dans l'outil proposé, lequel pourrait facilement être implémenté au moyen d'un item déjà homologué;
- la soumission contient des erreurs ou n'est pas conforme aux spécifications normatives ou à la norme JPSEC;
- la description technique n'est pas suffisante;
- les conditions de confidentialité ne sont pas appropriées.

7.6 Attribution d'identificateurs et enregistrement de définitions d'objet

Le processus de révision et la syntaxe ci-dessus garantissent que l'identificateur attribué est unique dans le registre et que le même identificateur n'est pas attribué à un autre objet.

Une fois l'attribution effectuée, l'identificateur et les informations associées doivent être inclus dans le registre et l'organisme d'enregistrement JPSEC doit informer le demandeur de cette attribution dans les neuf mois.

La définition d'outil JPSEC doit être consignée dans le registre au moment où l'identificateur est attribué.

7.6.1 Réutilisation d'identificateurs

Les identificateurs peuvent être réutilisés par un organisme d'enregistrement. Par exemple, les identificateurs deviennent disponibles pour réutilisation après leur expiration ou quand ils sont abandonnés volontairement ou recyclés.

Les propriétaires d'identificateur peuvent abandonner volontairement leur identificateur au moyen d'un demande de mise à jour.

7.6.2 Recyclage

Un organisme d'enregistrement JPSEC peut recycler un identificateur pour des raisons techniques ou pour mauvais usage de l'outil. Quand cela se produit, le propriétaire de l'identificateur en sera averti par une notification de mise à jour.

7.7 Maintenance

Aux fins de la maintenance du registre, un organisme d'enregistrement JPSEC doit implémenter des mécanismes permettant de conserver l'intégrité du registre y compris une sauvegarde adéquate afin de conserver des archives.

Un propriétaire d'identificateur peut mettre à jour les informations associées à l'outil JPSEC au moyen d'une demande de mise à jour.

Un organisme d'enregistrement JPSEC doit offrir des mécanismes permettant de conserver la confidentialité des entrées comme convenu dans la demande.

7.8 Publication du registre

Généralement, les intérêts de la communauté des utilisateurs des techniques de l'information sont servis au mieux si les informations d'enregistrement sont rendues publiques. Dans certains cas cependant, il peut y avoir une exigence de confidentialité concernant tout ou partie des données relatives à un enregistrement particulier, soit à titre permanent ou pour certaines portions du processus d'enregistrement.

Un organisme d'enregistrement JPSEC doit publier les informations d'enregistrement d'une façon qui soit cohérente avec les exigences de confidentialité de l'outil JPSEC.

Lorsque la publication est requise, les versions électronique et imprimée sur papier sont obligatoires. Si un organisme d'enregistrement JPSEC doit assurer la publication, il doit conserver des archives de distribution précises concernant ses publications.

7.9 Exigences relatives aux informations enregistrées

L'organisme d'enregistrement JPSEC doit publier électroniquement la liste des outils JPSEC non normatifs contenus dans son registre, ainsi que les informations y associées, d'une façon qui soit cohérente avec les exigences de confidentialité de l'outil JPSEC.

Les informations suivantes doivent être contenues dans le registre pour chaque outil JPSEC:

- l'identificateur attribué;
- nom du demandeur initial;
- adresse du demandeur initial;
- date de l'attribution originale;
- date du dernier transfert d'attribution, si autorisé (renouvelable);
- nom du propriétaire actuel (renouvelable);
- adresse du propriétaire actuel (renouvelable);
- nom, titre, adresse postale/électronique, numéro de téléphone/télécopie d'un personne de contact dans l'organisation (renouvelable);
- date de la dernière mise à jour (renouvelable);

Il doit également contenir les informations fournies par le demandeur sur son outil JPSEC comme spécifié dans le § 7.3 ainsi que les informations d'homologation.

Annexe A

Directives et cas de figure

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

A.1 Classe d'applications JPSEC

A.1.1 Introduction

Le présent paragraphe donne une description théorique de la façon dont une classe d'applications JPSEC peut être implémentée. Cette classe d'application représente des exemples de scénarios de distribution sécurisée d'images JPEG 2000. Les paragraphes ci-dessous offrent un aperçu général d'une application JPSEC théorique, y compris les entités JPSEC et les informations qui sont communiquées entre elles. Cette description est théorique et ne vise ni à définir une implémentation concrète ni à spécifier des exigences d'implémentation. Les applications spécifiques peuvent ou non comprendre les entités identifiées dans la description ci-dessous.

A.1.2 Aperçu général d'une distribution sécurisée d'images JPEG 2000

La Figure A.1 montre un aperçu général de la classe d'applications JPSEC de distribution sécurisée d'images JPEG 2000. Dans ces applications, l'application JPSEC peut être tenue d'offrir divers services de sécurité pour les images JPEG 2000, p. ex., la confidentialité de l'échange d'images ainsi que l'authentification de l'origine et du contenu d'image.

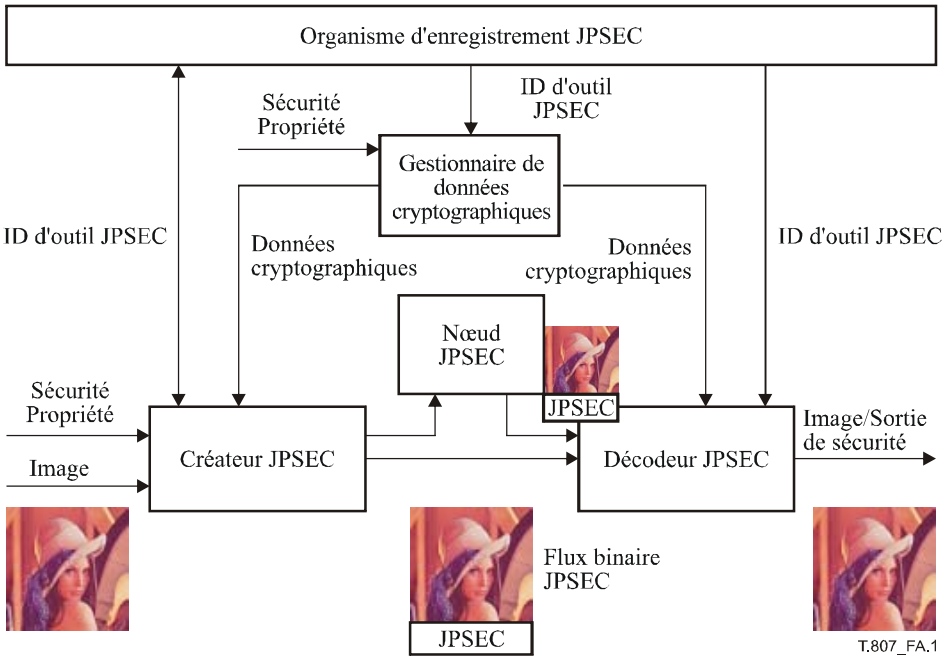


Figure A.1 – Aperçu général d'une application de distribution sécurisée d'images JPEG 2000

Dans l'application de distribution sécurisée d'images JPEG 2000, on peut identifier les étapes suivantes:

Etape 1: un flux à codage JPSEC est créé par un créateur JPSEC.

Etape 2: le flux à codage JPSEC est distribué par certain(s) nœud(s) JPSEC.

Etape 3: le flux à codage JPSEC est reçu et consommé puis est restitué par un consommateur JPSEC.

Etape 1: création du flux à codage JPSEC

Le créateur est chargé de créer le flux à codage JPEG 2000 sécurisé. Ce flux codé peut être créé à partir de données de phototrame ou à partir de données JPEG 2000 comprimées. Un créateur JPSEC applique diverses techniques de sécurité telles que le chiffrement, la production de signature et la production d'une valeur de contrôle d'intégrité (ICV, *integrity check value*) selon les données d'image.

Afin de sécuriser les données d'image, le créateur définit quelle propriété paramétrique de sécurité est associée à l'image. Une "propriété paramétrique de sécurité" contient les attributs suivants:

- zone d'influence (aire d'application de chaque méthode de protection);
- domaine de traitement (domaine qui doit être traité par chaque méthode de protection);
- granularité (unité de chaque méthode de protection);
- identification d'outil JPSEC (algorithme cryptographique appliqué et paramètres associés).

Etape 2: acheminement du flux à codage JPSEC

Un flux à codage JPSEC peut être transféré directement à un consommateur JPSEC via un réseau ou un média (comme un CD-ROM). Il peut également être transféré indirectement au moyen d'un nœud JPSEC pouvant appliquer au flux à codage JPSEC divers types de traitement additionnel, comme un transcodage.

Quand cela est requis par les méthodes de l'outil de sécurité JPSEC contenues dans le paramètre de propriété de sécurité du flux à codage JPSEC (p. ex. pour chiffrement ou pour authentification), le créateur JPSEC doit distribuer au consommateur JPSEC les données cryptographiques correspondantes au moyen d'un canal indépendant ('secret'). Ces données, telles que clé ou signature numérique, peuvent être gérées manuellement ou automatiquement par un gestionnaire de données cryptographiques.

Etape 3: restitution de la consommation d'un flux à codage JPSEC

Un flux à codage JPSEC est soumis à un traitement de consommateur JPSEC conformément à la propriété paramétrique de sécurité appliquée: cela implique l'application de techniques de sécurité appropriées, telles que le déchiffrement, l'authentification et le contrôle d'intégrité. Par ailleurs, pour chaque méthode de sécurité d'outil JPSEC, un créateur JPSEC et un consommateur JPSEC peuvent utiliser divers types de données cryptographiques.

Une sortie de données d'image déchiffrées et/ou de sécurité, telle qu'un résultat de vérification, est produite en tant que sortie du consommateur JPSEC.

Un créateur JPSEC, un consommateur JPSEC et un gestionnaire de données cryptographiques peuvent consulter l'organisme d'enregistrement JPSEC afin d'obtenir les instructions de traitement nécessaires à un identificateur d'outil JPSEC spécifique.

Les paragraphes suivants décrivent plus en détail une entité JPSEC théorique, conformément à un service JPSEC. La Figure A.2 montre la légende descriptive à utiliser.

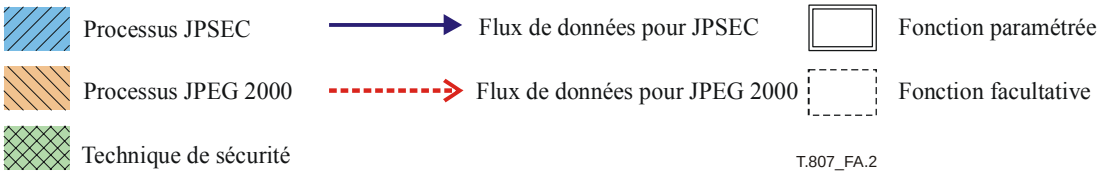


Figure A.2 – Légende descriptive

- **processus JPSEC**: processus qui utilise les outils définis dans la présente Recommandation | Norme internationale.
- **processus JPEG 2000**: processus défini dans la Rec. UIT-T T.800 | ISO/CEI 15444-1 (Partie 1 de la norme JPEG 2000).
- **technique de sécurité**: technique de sécurité bien connue, définie soit dans la présente Recommandation | Norme internationale ou dans une autre norme ou Recommandation.
- **flux de données pour JPSEC**: flux de données qui communique des informations définies dans la présente Recommandation | Norme internationale. Une ligne discontinue indique des informations facultatives.
- **flux de données pour JPEG 2000**: flux de données défini dans la Rec. UIT-T T.800 | ISO/CEI 15444-1 (Partie 1 de la norme JPEG 2000).
- **fonction paramétrée**: fonction qui possède plusieurs variantes qui peuvent être sélectionnées par une application.
- **fonction facultative**: fonction qui peut être appliquée à titre facultatif dans une application JPSEC.

A.1.3 Procédure de description de fin de chiffrement

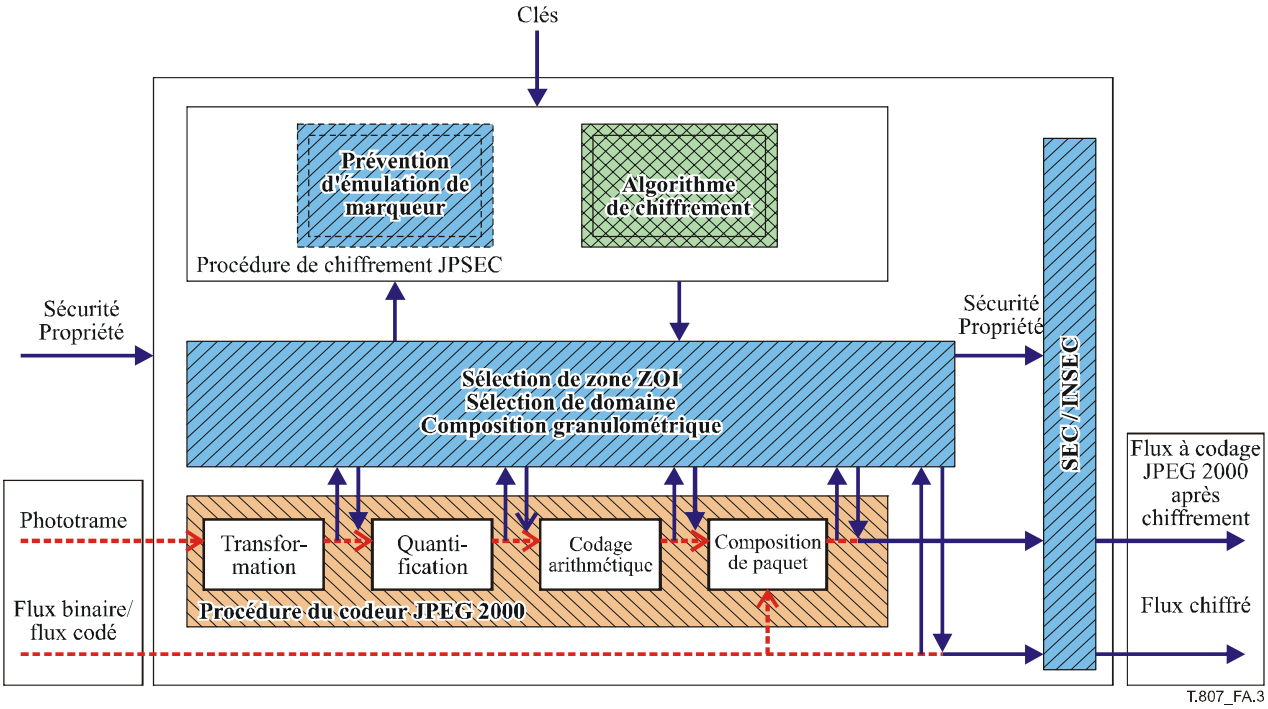


Figure A.3 – Procédure de chiffrement

La Figure A.3 ci-dessus montre l'aperçu général d'un exemple de procédure de chiffrement pour un créateur JPSEC. Cette procédure contient les traitements suivants:

- extraction de données conformément au domaine de traitement spécifié;
- sélection d'une portion de données récupérées conformément à la zone d'influence spécifiée (c'est-à-dire chiffrement partiel);
- chiffrement des données sélectionnées au moyen de la technique de sécurité spécifiée. Par ailleurs, il est possible de chiffrer les données dans une unité en fonction de la granularité. Dans ce cas, différentes clés peuvent être utilisées pour différentes unités.
- remplacer les données en clair par les données chiffrées;
- (facultativement) appliquer un mécanisme de prévention d'émulation de marqueur;
- composer la propriété paramétrique de sécurité dans le segment marqueur SEC et/ou INSEC.

Noter qu'en général la procédure de chiffrement JPSEC produit un flux à codage JPSEC qui n'est pas rétrocompatible avec la Partie 1 de la norme JPEG 2000. Les données d'image sont destinées à être transmises à un décodeur conforme à la Partie 1 après déchiffrement approprié. Il est possible d'appliquer un mécanisme de prévention d'émulation de marqueur afin d'éviter une émulation de segment marqueur dans le flux codé par chiffrement.

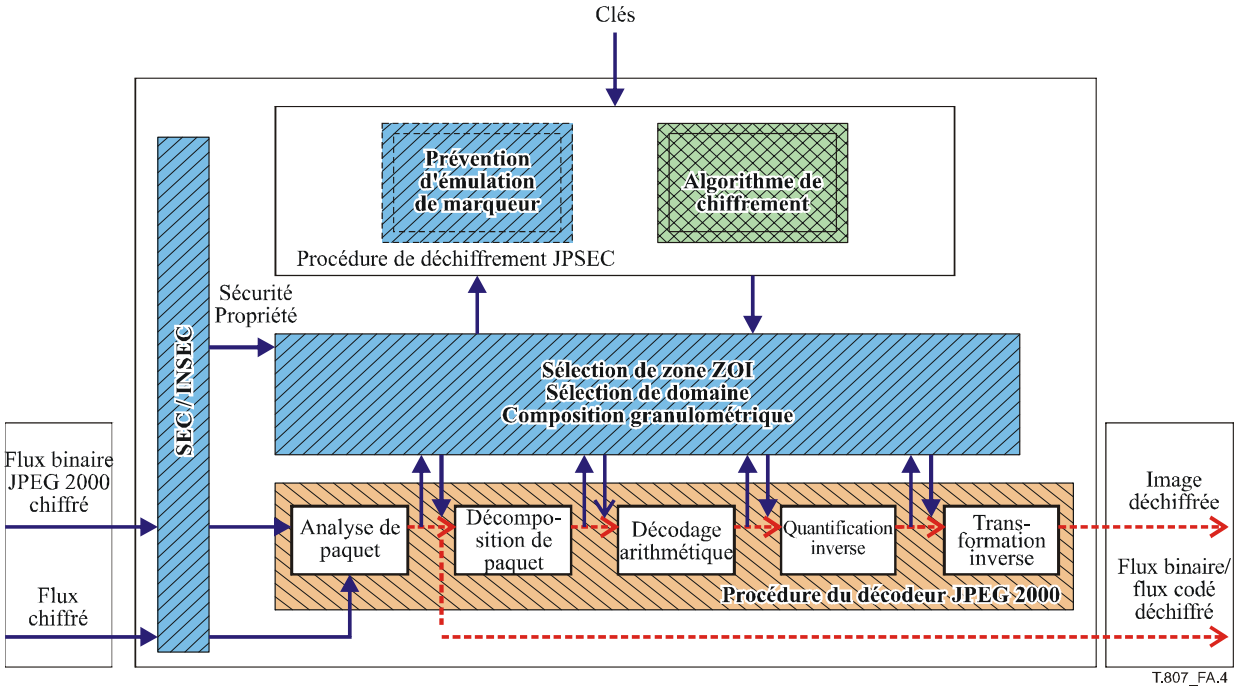


Figure A.4 – Procédure de déchiffrement

La Figure A.4 ci-dessus montre l'aperçu général d'un exemple de procédure de déchiffrement pour un consommateur JPSEC. Cette procédure contient les traitements suivants:

- analyse de la propriété paramétrique de sécurité dans le segment marqueur SEC et/ou INSEC;
- extraction de données conformément au domaine de traitement signalé;
- sélection d'une portion des données récupérées conformément aux clés à conserver (c'est-à-dire déchiffrement partiel)
- déchiffrement des données sélectionnées au moyen d'une technique de sécurité signalée. Par ailleurs, il est possible de déchiffrer les données d'une unité sur la base de la granularité;
- remplacement des données chiffrées par les données déchiffrées;
- application d'un mécanisme de prévention d'émulation de marqueur, si ce mécanisme a été appliqué pendant le processus de chiffrement.

A.1.4 Procédure de production et d'authentification de signature

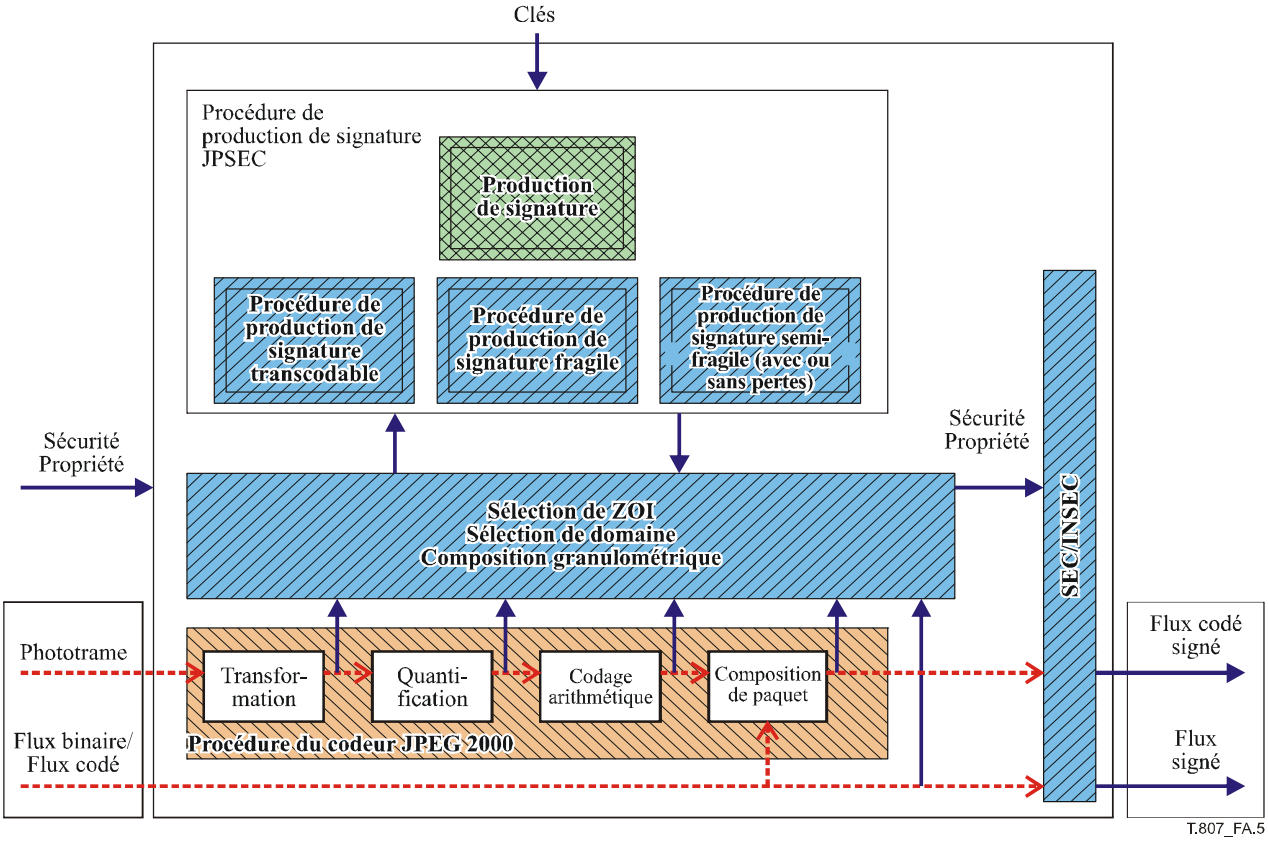


Figure A.5 – Procédure de production de signature

La Figure A.5 ci-dessus montre l'aperçu général d'un exemple de procédure de production de signature pour un créateur JPSEC. Cette procédure contient les traitements suivants:

- extraction de données conformément au domaine de traitement spécifié;
- sélection d'une portion des données récupérées conformément à la zone d'influence spécifiée (c'est-à-dire signature partielle);
- calcul des signatures numériques correspondant aux données sélectionnées au moyen de la technique de sécurité spécifiée. Par ailleurs, il est possible de produire les signatures numériques d'une unité en fonction de la granularité;
- composition de la propriété paramétrique de sécurité, y compris les signatures numériques calculées, dans le segment marqueur SEC et/ou INSEC.

Noter que, dans le modèle JPSEC, trois modes d'authentification sont définis: "mode fragile", "mode semi-fragile (avec pertes/sans pertes)" et "mode transcodable". Une authentification en "mode fragile" peut détecter toute modification d'élément binaire dans un flux codé, alors que l'authentification en mode "semi-fragile" peut détecter tout essai de détection intentionnelle mais ne peut résister à une distorsion occasionnelle que jusqu'à une limite prédéterminée. Par ailleurs, une authentification en "mode de transcodage" peut vérifier la partie originelle du flux codé.

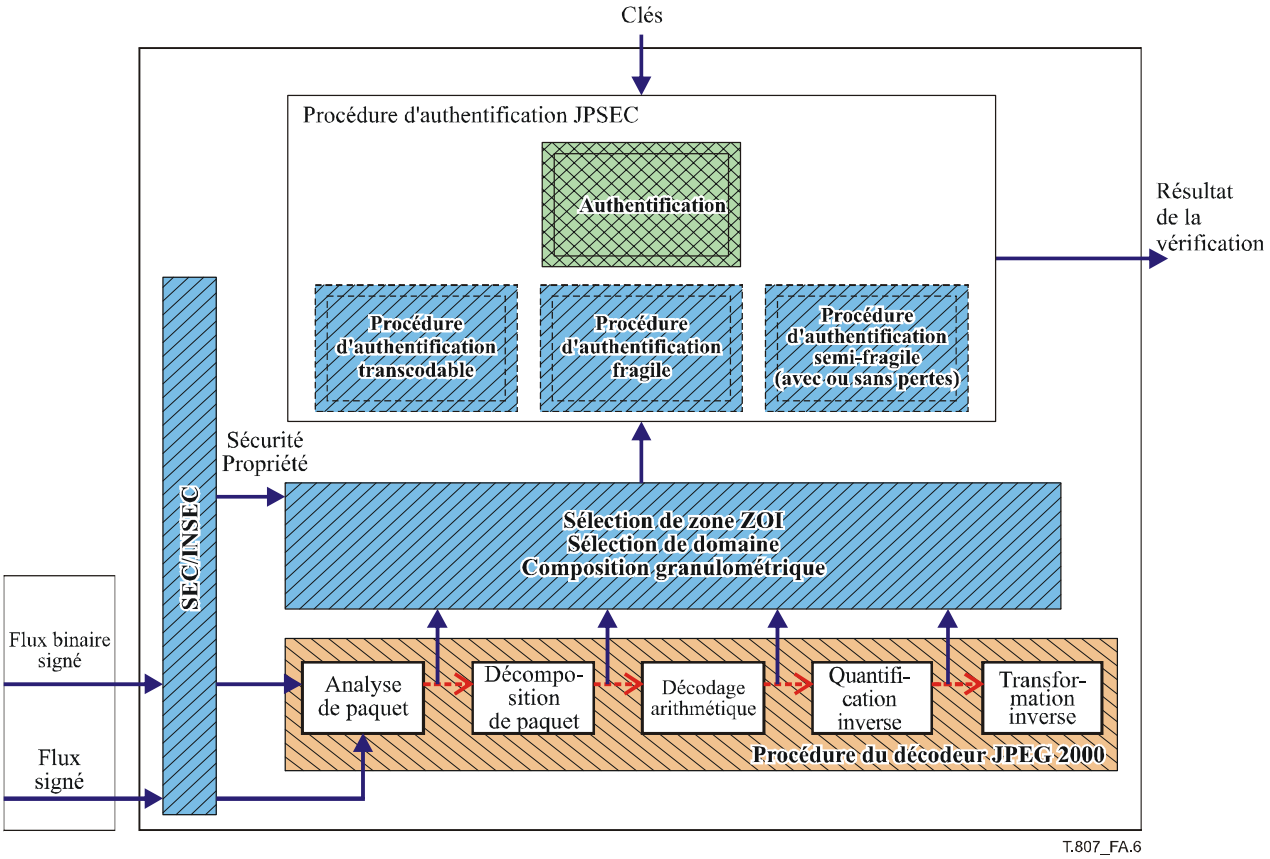


Figure A.6 – Procédure d'authentification

La Figure A.6 ci-dessus montre l'aperçu général d'un exemple de procédure d'authentification pour un consommateur JPSEC. Cette procédure contient les traitements suivants:

– extraction de données d'un domaine de traitement signalé;

– sélection d'une portion de données récupérées conformément à la zone d'influence signalée;

– vérification des données sélectionnées au moyen de la technique de sécurité signalée. Par ailleurs, il est possible de vérifier les données sélectionnées d'une unité en fonction de la granularité.

A.1.5 Procédure de production et de contrôle de valeur ICV (valeur de contrôle d'intégrité)

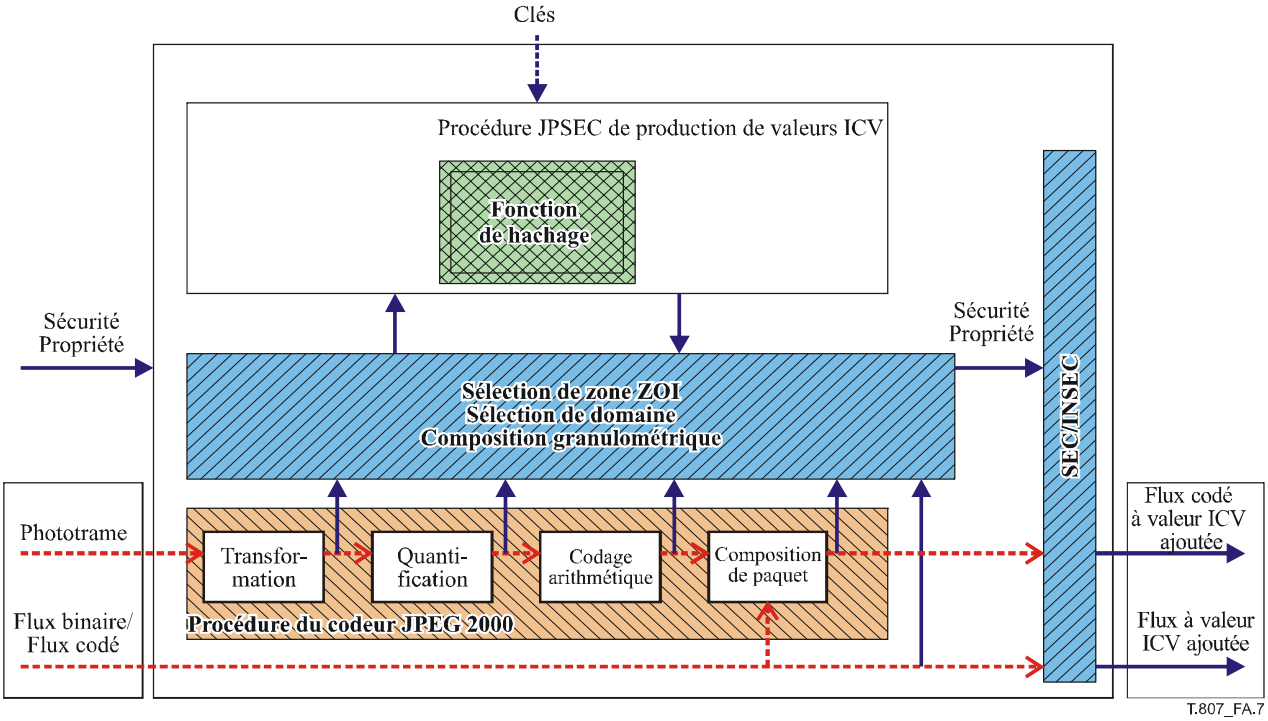


Figure A.7 – Procédure de production de valeur ICV (valeur de contrôle d'intégrité)

La Figure A.7 ci-dessus montre l'aperçu général d'un exemple de procédure de production de valeur ICV pour un créateur JPSEC. Cette procédure contient les traitements suivants:

- extraction de données dans un domaine de traitement spécifié;
- sélection d'une portion de données récupérées conformément à la zone d'influence spécifiée;
- calcul des valeurs ICV correspondant aux données sélectionnées au moyen de la technique de sécurité spécifiée. Par ailleurs, il est possible de produire les valeurs ICV d'une unité en fonction de la granularité;
- composition de la propriété paramétrique de sécurité, y compris les valeurs ICV calculées, d'un segment marqueur SEC ou INSEC.

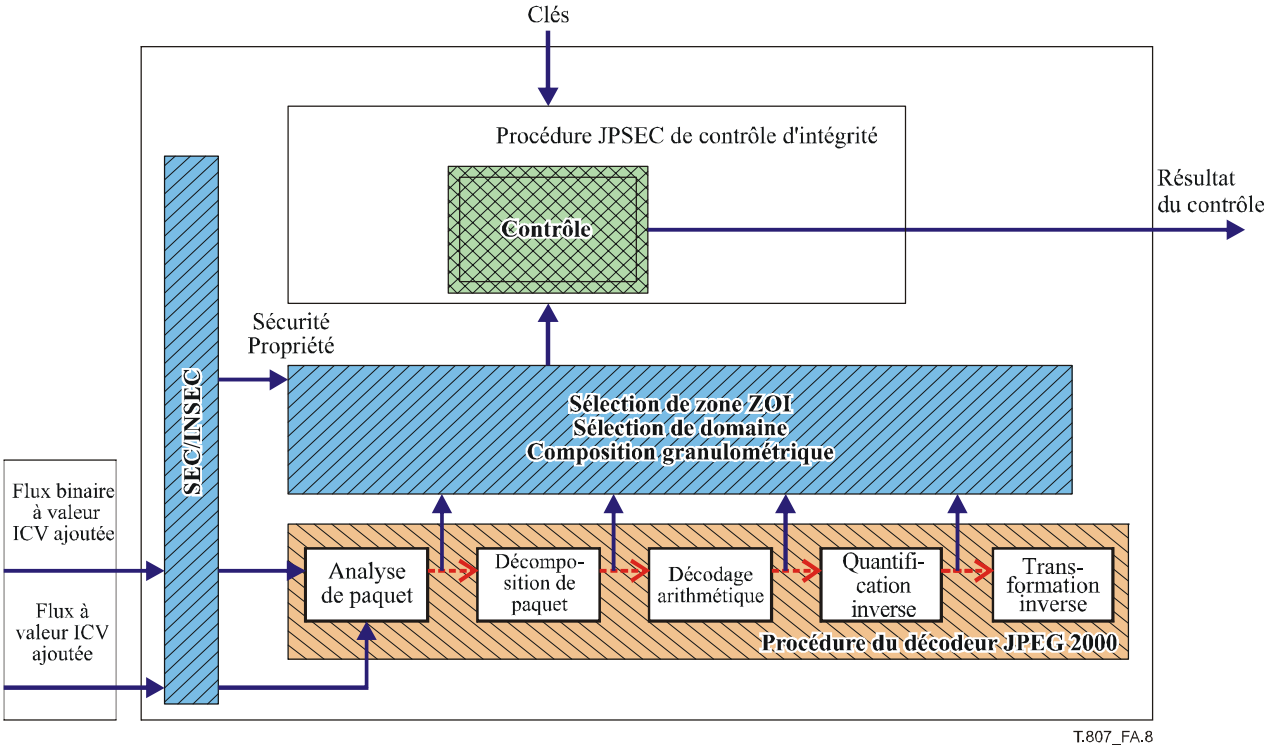


Figure A.8 – Procédure de contrôle d'intégrité

La Figure A.8 ci-dessus montre l'aperçu général d'un exemple de procédure de contrôle d'intégrité pour un consommateur JPSEC. Cette procédure contient les traitements suivants:

– extraction de données conformément au domaine de traitement signalé;

– sélection d'une portion des données récupérées conformément à une zone d'influence signalée;

– vérification des données sélectionnées au moyen d'une technique de sécurité signalée. Par ailleurs, il est possible de vérifier les données sélectionnées d'une unité en fonction de la granularité.

Annexe B

Exemples de technologie

(La présente annexe fait partie intégrante de la présente Recommandation | Norme internationale)

B.1 Introduction

La syntaxe JPSEC permet d'appliquer des outils de sécurité normatifs et non normatifs à des images JPEG 2000. Le présent paragraphe décrit dix exemples informatifs de technologie qui démontrent différents usages de la syntaxe JPSEC. Ces exemples, purement informatifs, ne sont pas pris en compte par la norme JPSEC mais sont présentés afin d'en démontrer la flexibilité.

Ces exemples de technologie sont les suivants:

- un procédé de contrôle d'accès flexible pour JPEG 2000;
- un cadre unifié d'authentification pour images JPEG 2000;
- une méthode simple de chiffrement en mode paquet pour flux à codage JPEG 2000;
- un outil de chiffrement pour contrôle d'accès JPEG 2000;
- un outil de production de clés pour contrôle d'accès JPEG 2000;
- un brassage par ondelette et par domaine de flux binaire pour contrôle d'accès conditionnel;
- un accès progressif pour flux à codage JPEG 2000;
- une authenticité modulable des flux à codage JPEG 2000;
- une confidentialité des données JPEG 2000 et un système de contrôle d'accès fondé sur le découpage et le masquage de données;
- un flux direct à échelonnement et transcodage sécurisés.

B.2 Procédé de contrôle d'accès flexible pour flux à codage JPEG 2000

B.2.1 Service de sécurité

Un procédé de contrôle d'accès permet la restitution de flux à codage JPEG 2000 conformément à toute combinaison de résolutions, couches qualitatives, pavés et districts.

B.2.2 Application typique

Ce procédé assure la protection de la remise du contenu via divers supports, p. ex. Internet, télévision numérique par câble, télédiffusion par satellite et CD-ROM. Généralement, la technologie est viable dans les applications où un flux codé n'est chiffré qu'une seule fois du côté de l'éditeur mais où le flux codé protégé est déchiffré de nombreuses façons selon les différents privilèges acquis du côté de l'utilisateur.

B.2.3 Motivation

Dans le modèle de superdistribution, l'éditeur distribue librement le contenu protégé et de façon sûre les clés de ce contenu. Un utilisateur qui désire avoir accès à des portions d'un flux codé envoie sa requête au serveur de clés, lequel, à son tour, répond avec les clés de déchiffrement appropriées conformément au privilège de l'utilisateur. Celui-ci peut alors accéder aux sous-images autorisées.

B.2.4 Aperçu technique

L'éditeur produit un flux JPEG 2000 codé et protégé en chiffrant chaque paquet. Le noyau de la technologie est la façon de gérer un arbre de clés qui est construit dans un ordre quelconque de pavés, de composantes, de résolutions, de couches, de districts et même de blocs de code. Afin de faciliter la description de la technologie, l'on part du principe que l'ordre hiérarchique des clés est RLCP (résolution-couche-composante-district) et que chaque résolution possède le même nombre de districts. Ci-dessous, on admet une fonction de hachage unilatérale h(.) et un flux codé d'images JPEG 2000 avec n_T pavés, n_C composantes, n_L couches, n_R résolutions par composante de pavé, n_P districts par résolution. Avec une clé principale K pour un flux à codage JPEG 2000, l'on construit un arbre de clés comme suit.

1) Produire une clé $k^t = h(K\,|"T"|t)$, pour chaque pavé $t = 0,1, \ldots, n_T-1$, où "|" est la concaténation et où *"T"* désigne le code ASCII de la lettre *T*.

2) Produire une clé $k^r = h(k^{r+1})$, pour chaque $r = n_R-2, \ldots, 1, 0$, où $k^{n_R-1} = h(k^t\,|"R")$ et où "*R*" désigne le code ASCII de la lettre *R*.

3) Calculer une clé $k^{rl} = h(k^{r(l+1)})$, pour chaque $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 2, \ldots, 1, 0$, où $k^{r(n_L-1)} = h(k^r|"L")$ et où "*L*" désigne le code ASCII de la lettre *L*.

4) Calculer une clé $k^{rlc} = h(k^{rl}|"C"|c)$, pour chaque $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 1, \ldots, 1, 0$, $c = 0, 1, \ldots, n_C - 1$, où "*C*" désigne le code ASCII de la lettre *C et c* désigne l'indice de ce composant.

5) Produire des clés $k^{rlcp} = h(k^{rlc}|"P"|p)$, pour chaque $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 1, \ldots, 1, 0$, $c = 0, 1, \ldots, n_C - 1$, $p = 0, 1, \ldots, n_R - 1$, où "*P*" désigne le code ASCII de la lettre *P* et où *p* désigne l'indice de ce district.

Le flux codé et protégé est produit par chiffrement de chaque corps de paquet au moyen de sa clé correspondante (qui est une feuille dans l'arbre des clés).

Afin de restituer une sous-image à partir d'un flux codé et protégé, un utilisateur obtient les clés d'accès correspondantes (p. ex., octroyées à partir d'un serveur de clés). Ces clés d'accès permettent de reconstituer exactement les feuilles de l'arbre de clés correspondant aux paquets de la sous-image demandée. Le processus de reconstruction de clé est similaire à celui de la production par un arbre de clés. Les feuilles servent à déchiffrer les paquets correspondants.

B.2.5 Syntaxe du flux codé

Le Tableau B.1 décrit la structure du segment marqueur SEC. Le champ *ZOI* signale les paramètres octroyés, le champ P_{ID} signale les paramètres de la méthode de protection pour ce procédé de contrôle d'accès. Le champ PM_{ID} est toujours réglé à 1 afin d'indiquer que le modèle de déchiffrement est utilisé. Le champ TP_{ID} signale les paramètres additionnels pour ce procédé de contrôle d'accès. *KTO* est l'ordre de production d'un arbre de clés. Le champ L_{aki} indique la longueur des informations sur les clés d'accès.

Tableau B.1 – Exemples de paramètres pour ce procédé

t	i	ID_{RA}	L_{ZOI}	ZOI	L_{PID}	P_{ID}

Paramètre		Longueur (bits)	Valeurs	Signification
t		8 (FBAS)	1	Outil de protection de l'organisme d'enregistrement
i		8 (RBAS)	*Valeur d'instance*	Identificateur d'instance d'outil
ID_{RA}	$ID_{RA,id}$	32	*Valeur d'ID d'outil*	Identificateurs enregistrés
	$ID_{RA,nsl}$	8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$	168	*Espace nominatif*	Espace nominatif de l'organisme auprès duquel cet outil est enregistré.
L_{ZOI}		16 (RBAS)	$[2 \ldots 2^{16} - 1]$	Longueur de zone ZOI.
ZOI		Variable	Voir § 5.7	Zone d'influence pour ce procédé
L_{PID}		16 (RBAS)	$[2 \ldots 2^{16} - 1]$	Longueur de $L_{PID} + P_{ID}$
P_{ID}		Variable	Voir Tableau B.2	Paramètres pour ce procédé

Tableau B.2 – P_{ID}

$PM_{ID} = 1$	T_{decry}	TP_{ID}

Paramètre	Longueur (bits)	Valeurs	Signification
$ID_T = 1$	8	Toujours réglé à 1	Balise pour modèle de déchiffrement
T_{decry}	Variable	Valeurs du modèle de déchiffrement	Modèle de déchiffrement
TP_{ID}	Variable	Voir Tableau B.3	Informations additionnelles pour ce procédé

Tableau B.3 – TP_{ID}

KTO	L_{aki}	AK_{Info}

Paramètre	Longueur (bits)	Valeurs	Signification
KTO	8	0 ... (2^8–1)	Ordre de l'arbre de clés, qui peut être différent de l'ordre de progression du flux codé, provisoirement, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL autres valeurs: réservé
L_{aki}	16	0 ... (2^{16}–1)	Longueur des informations d'accès aux clés, si L_{aki} = 0, aucun fichier AK_{Info} n'est présenté.
AK_{Info}	Variable	Voir Tableau B.4	Informations sur la clé d'accès (p. ex. longueur de clé, nombre de clés)

Tableau B.4 – AK_{info}

L_{uk}	UK	E_{ak}	N_{ak}	AK

Paramètre	Longueur (bits)	Valeurs	Signification
L_{uk}	16	0 ... (2^{16}–1)	Longueur de la clé d'utilisateur
UK	L_{uk}	NaN	Informations de l'utilisateur sur les clés
E_{ak}	16	Voir Tableau 24	Algorithme servant à chiffrer les clés d'accès
N_{ak}	16	0 ... (2^{16}–1)	Nombre de clés d'accès
AK	N_{ak} * K_{bc}	NaN	Clés d'accès

B.2.6 Conclusion

Cette technologie permet à un éditeur de protéger un flux à codage JPEG 2000 avec une clé principale. Le flux codé et protégé est autorisé à être remis à un nombre quelconque d'utilisateurs, mais les clés des paquets sont gardées secrètes. Le serveur distant de clés produit différentes clés d'accès pour les utilisateurs conformément à leurs priorités. Les utilisateurs produisent les clés de paquet octroyées à partir de leurs clés d'accès et obtiennent différentes images octroyées. En d'autres termes, la technologie possède la propriété appelée "*chiffrer une fois, accéder de nombreuses façons*".

B.3 Cadre unifié d'authentification pour images JPEG 2000

B.3.1 Description opérationnelle

Cet outil JPSEC fournit les services JPSEC suivants: vérification de l'intégrité des données d'image/du contenu et authentification de la source, c'est-à-dire authentification fragile/semi-fragile pour images JPEG 2000, fondée sur des procédés de signature numérique.

Comme cet outil prend en charge les authentifications aussi bien fragiles que semi-fragiles, il peut être utilisé dans différents scénarios d'application, y compris la distribution d'image, le flux direct d'images, l'imagerie médicale et militaire, la police, le commerce électronique et l'administration publique en ligne.

Dans un environnement diffus, les images pourraient rencontrer diverses sortes de distorsion occasionnelle comme le transcodage et la conversion de format. Les techniques d'authentification traditionnelles de type cryptographique protègent les images JPEG 2000 au niveau de l'intégrité des données et ne peuvent pas résister à ces types de distorsion qui préservent le contenu. Des techniques d'authentification semi-fragiles sont donc requises afin de protéger les images JPEG 2000 au niveau du contenu d'image. Cet outil unifie aussi bien l'authentification des données d'image que celle du contenu d'image. Cet outil propose un nouveau concept appelé *plus bas débit d'authentification* (LABR, *lowest authentication bit rate*). C'est-à-dire que si l'image est transcodée à un débit qui n'est pas inférieur au débit LABR, elle le sera en tant qu'image authentique; si ce n'est pas le cas, elle le sera en tant qu'image non authentique. L'authentification peut être fragile ou semi-fragile. Dans l'authentification semi-fragile, l'outil est en mesure d'identifier l'endroit où l'altération a eu lieu quand l'image est jugée non authentique.

B.3.2 Aperçu technique

Afin d'offrir l'authentification fragile et semi-fragile, un groupe de techniques a été appliqué dans cet outil JPSEC informatif. Ce groupe comprend la sélection des caractéristiques, la signature numérique, le masquage des données avec et sans pertes et les codes de correction d'erreur (ECC). Conformément au débit LABR spécifié par les utilisateurs, les caractéristiques correspondantes sont sélectionnées sur la base d'une analyse appliquée à la structure JPEG 2000: la signature numérique est alors produite. Pour l'authentification semi-fragile, le code ECC est utilisé afin d'augmenter le niveau de robustesse. Les bits de contrôle de parité (PCB, *parity check bit*) sont imbriqués dans l'image en filigrane afin d'identifier les emplacements de l'attaque. L'imbrication de données peut être effectuée de deux façons différentes: avec pertes et sans pertes. Dans le masquage des données avec pertes, l'image originale ne peut pas être récupérée après le masquage des données. Dans le masquage des données sans pertes, d'autre part, l'image est modifiée de façon réversible, c'est-à-dire que l'image originale peut être récupérée si l'image marquée n'a pas été altérée. L'authentification semi-fragile sans pertes est utile pour la norme JPEG 2000 car celle-ci prend en charge la compression du format avec pertes en format sans pertes. Elle est particulièrement utile aux applications d'imagerie médicale locale et distante, où le format sans pertes est une exigence essentielle.

De même que le débit binaire de compression d'image sert à commander et à caractériser le taux de compression, le paramètre de débit LABR (plus bas débit d'authentification) sert à commander quantitativement le taux de protection. Par exemple, quand une image JPEG 2000 est protégée à un débit LABR de 2 bpp (bits par pixel), toute version transcodée de l'image sera restituée comme authentique par le système proposé tant que le débit après transcodage sera supérieur ou égal à 2 bpp.

La Figure B.1 décrit comment l'outil peut servir à protéger des images.

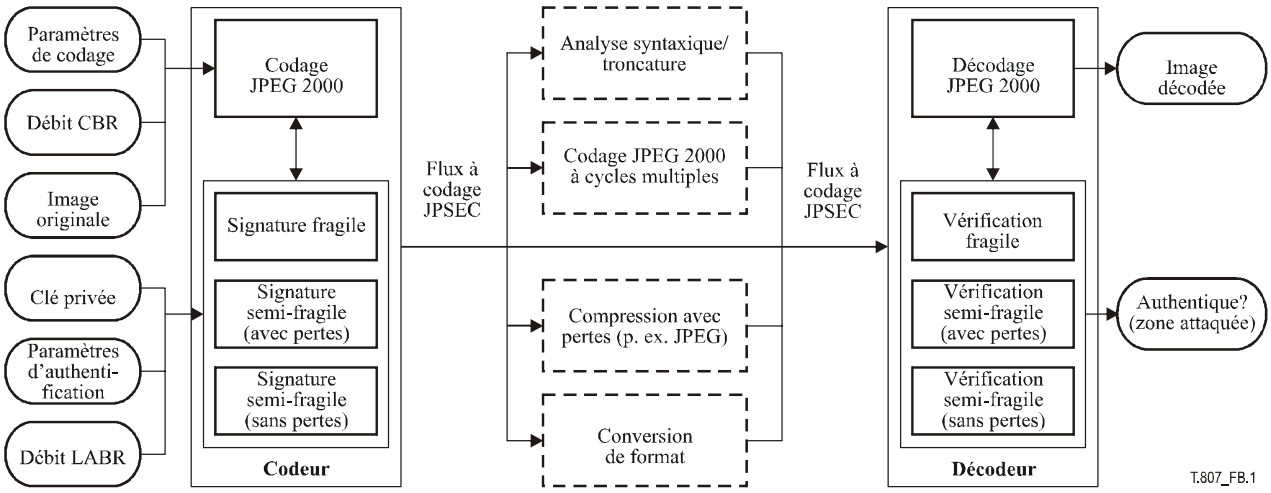


Figure B.1 – Protection d'image utilisant le cadre unifié d'authentification pour JPEG 2000

Cet outil peut utiliser différentes syntaxes de signalisation selon la méthode d'authentification choisie. Pour l'authentification fragile, cet outil utilise la syntaxe d'outil JPSEC normatif, comme défini dans le § 5.8.3. Pour l'authentification semi-fragile, il utilise la syntaxe d'outil JPSEC non normatif, comme illustré dans le Tableau B.5. En outre, le champ F_{INSEC} devrait être réglé à 0 car le marqueur INSEC n'est pas utilisé par cet outil et le champ F_{mod} devrait être réglé à 1 parce que le flux codé résultant de cet outil JPSEC reste conforme à la Partie 1 de la norme JPEG 2000.

Tableau B.5 – Syntaxe pour l'authentification semi-fragile

Paramètre				Longueur (bits)	Valeur	Signification déduite
t				8 (FBAS)	1	La syntaxe d'outil non normatif est utilisée
i				8 (RBAS)	0 ... (2^7 – 1)	Indice d'instance d'outil
ID_{RA}	$ID_{RA,id}$			32	0 ... (2^{32} – 1)	Numéro d'identification à recevoir du RA
	$ID_{RA,nsl}$			8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$			168	*espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
L_{ZOI}				16 (RBAS)	0 ... (2^{16} – 1)	Longueur de zone ZOI
ZOI				Variable	*Valeurs ZOI*	Zone couverte dans l'image protégée par l'outil
L_{PID}				16 (RBAS)	0 ... (2^{16} – 1)	Longueur de P_{ID} et L_{PID} en octets
P_{ID}	ID_T			8	2	Un modèle d'authentification est utilisé, comme défini dans le Tableau 21.
	T_{auth}	M_{auth}		8	2	Une méthode de signature numérique est utilisée, comme défini dans le Tableau 34.
		P_{auth}	M_{DS}	8	Voir Tableau 41	Un algorithme de signature numérique est utilisé, tel que DSA ou RSA.
			H_{DS}	8	Voir Tableau 37	Fonction de hachage utilisée
			KT_{DS}	Variable	*Valeurs du modèle de clé*	La clé publique est mémorisée dans KT_{DS}. Cet outil n'utilise qu'une seule clé publique
			SIZ_{DS}	16	0 ... (2^{16} – 1)	Longueur de la signature numérique en octets
	PD			1	0_b	La structure de segment FBAS est terminée
				1	0_b	Le domaine des pixels n'est pas utilisé
				1	0_b	Le domaine des coefficients d'ondelette n'est pas utilisé
				1	1_b	Le domaine des coefficients d'ondelette quantifiés est utilisé
				1	0_b	Le domaine du flux codé n'est pas utilisé
				3	000_b	Réservé pour utilisation par l'ISO
	G	PO		16	*Valeurs de l'ordre de traitement*	Ordre de traitement
		GL		8	0000 1001	Niveau de granularité: l'unité de protection est l'aire totale identifiée dans la zone ZOI
	V	N_V		16	1	Nombre de signatures numériques dans la liste: 1.
		S_V		8 (RBAS)	1 ... (2^8 – 1)	Longueur de la signature numérique en octets
		VL		8* S_V	*Valeur de signature numérique*	Signatures numériques produites par l'outil
	LABR	$LABR_{int}$		8	0 ... (2^8 – 1)	Partie entière de LABR
		$LABR_{fra}$		8	0 ... (2^8 – 1)	Partie fractionnaire de LABR
	Seuil			8	[0 ... 2^8 – 1]	Valeur du seuil (valide seulement pour authentification sans pertes)
	Brassage			8	[0 ... 2^8 – 1]	Nombre de brassages afin d'imbriquer des bits de filigrane (valide seulement pour l'authentification sans pertes)

L'unique identificateur de cet outil doit être attribué par l'organisme d'enregistrement. La description d'outil peut être importée par téléchargement à partir de l'organisme d'enregistrement (RA, *registration authority*) au moyen de l'identificateur attribué.

B.3.3 Conclusions

En résumé, cet outil a réalisé les caractéristiques spéciales suivantes:

- authentification des images JPEG 2000 au niveau des données d'image ou à celui du contenu d'image, en intégrant l'authentification fragile et l'authentification semi-fragile dans un même cadre. Par ailleurs, l'authentification semi-fragile contient les deux modes: avec et sans pertes.
- robustesse à l'égard de diverses distorsions occasionnelles comme celles qui sont introduites par transcodage, par conversion de format, compression avec pertes et codage à cycles multiples JPEG 2000. Cet outil peut donc servir à protéger les images JPEG 2000 dans un environnement diffus.
- protection modulable des images JPEG 2000. Spécifiquement, cet outil est en mesure de protéger tout pavé, composant, résolution, couche, district, ou bloc de code.
- compatibilité avec le cadre de sécurité des informations d'état de la technique, appelé *infrastructure de clés publique*s (PKI, *public key infrastructure*) qui constitue la base de normes internationales existantes, comme la Rec. UIT-T X.509.
- taux de protection quantitatif, contrôlé par un unique paramètre appelé *taux LABR*, qui apporte beaucoup de commodité aux utilisateurs ultimes.
- capacité à localiser les régions d'image éventuellement attaquées si l'image est jugée non authentique. Cette capacité pourrait aider à convaincre visuellement les utilisateurs.
- prise en charge de protection de la conversion du format avec pertes au format sans pertes, correspondant à la compression du format avec pertes en format sans pertes selon les normes de codage JPEG 2000. Cet outil possède donc des applications beaucoup plus étendues, y compris celles d'imagerie médicale locale et distante.

B.4 Méthode simple de chiffrement en mode paquet pour flux à codage JPEG 2000

B.4.1 Description opérationnelle

Le présent paragraphe présente une technique de chiffrement sélectif pour images JPEG 2000. Il est fondé sur un chiffrement au niveau des paquets et sur des algorithmes de chiffrement normalisés et robustes.

Le service de sécurité visé par cette technique est la confidentialité des images à codage JPEG 2000, qui est obtenue par chiffrement du flux codé. Par conséquent, la protection des droits IPR ainsi que la protection de la sphère privée peuvent être réalisées au moyen de cette technique.

La méthode prend en charge le transcodage, l'échelonnabilité et d'autres fonctionnalités de traitement de contenu sans devoir accéder à la clé cryptographique et sans devoir exécuter un déchiffrement suivi d'un rechiffrement. Cette méthode n'interfère pas avec le processus de codage et décodage. Son influence défavorable est très limitée sur l'efficacité de compression et inexistante sur la tolérance aux erreurs. Une telle méthode offre une flexibilité maximale lors de l'implémentation de scénarios et d'applications à divers niveaux de sécurité.

Cette technique peut être utilisée par les producteurs de contenu afin de limiter l'accès au contenu d'image ou par les fournisseurs de contenu afin de garantir une remise confidentielle du contenu aux utilisateurs ultimes.

B.4.2 Aperçu technique

Cette technique consiste à chiffrer le flux codé après compression de l'image, comme représenté dans la Figure B.2.

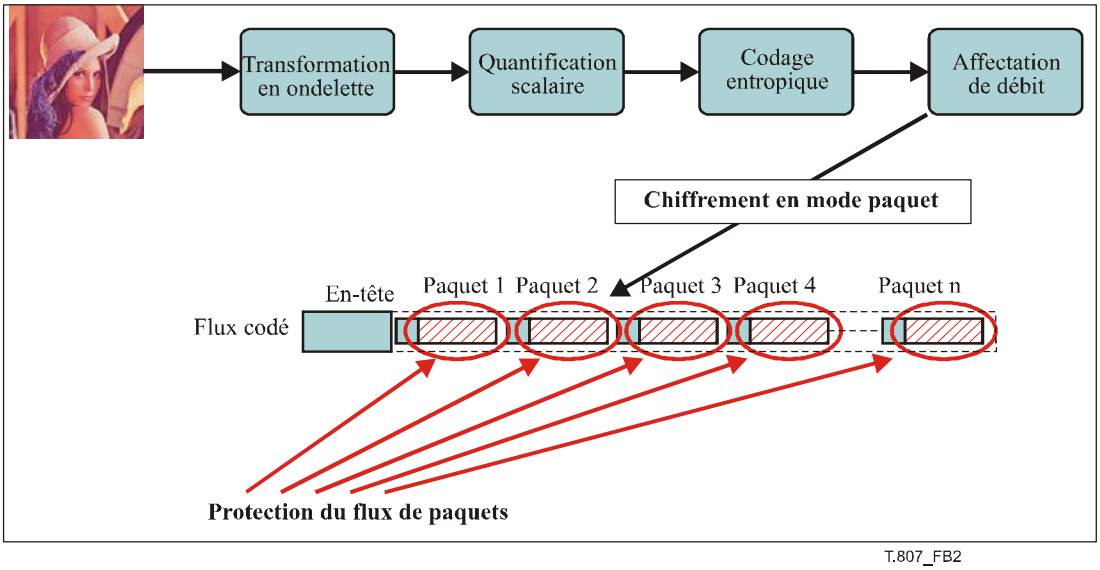


Figure B.2 – Principe du chiffrement en mode paquet

Cet outil JPSEC peut recevoir en entrée plusieurs paramètres associés à l'image: niveaux de résolution, couches qualitatives, composantes, districts ou pavés. Seules les charges utiles de paquet correspondant à ces paramètres d'entrée sont alors traitées. Le flux codé et protégé conserve donc une structure JPEG 2000 normale. Une fois que le flux codé a été chiffré, le segment marqueur SEC est ajouté à l'en-tête principal afin de permettre à tout consommateur JPSEC de déchiffrer correctement l'image ultérieurement.

Cette méthode utilise des algorithmes sous-jacents connus et normalisés afin de chiffrer sélectivement les paquets: il s'agit des algorithmes DES ou AES, associés aux modes normalisés décrits dans la référence [22], comme ECB, CBC, CFB, OFB et CTR. Tout autre algorithme de chiffrement par blocs pourrait évidemment être utilisé: les méthodes DES et AES sont données ici comme exemples d'algorithmes de chiffrement normalisés.

B.4.2.1 Exemple de signalisation

La technique peut être signalée dans la syntaxe fondée sur le modèle figurant dans le paragraphe normatif. On trouvera ci-dessous un exemple de signalisation pour cette technique (voir le Tableau B.6), qui spécifie une seule zone pour le paramètre ZOI, mais évidemment il pourrait y en avoir plus, suivant la même syntaxe que Zone^0.

Tableau B.6 – Exemple de zone d'influence, avec coordonnées spatiales, résolutions et couches

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NZzoi			8	1 (RBAS)	Nombre de zones égal à 1
Zone^0	DCzoi		1	0	Le segment verrouillé en octets ne suit pas
			1	0	Classe de description associée à l'image
			6	101100	Régions d'image, niveaux de résolution, couches qualitatives et composantes sont spécifiés dans l'ordre
	Pzoi^1	Mzoi^1	1	0	Le segment verrouillé en octets ne suit pas
			1	0	Les zones spécifiées sont influencées par la méthode de protection
			1	0	Un item unique est spécifié
			2	00	Mode rectangulaire
			2	00	Izoi utilise 8 bits pour un entier
			1	1	Izoi est décrit dans deux dimensions

Tableau B.6 – Exemple de zone d'influence, avec coordonnées spatiales, résolutions et couches

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
		Izoi[1]	8	0110 0100	Xul est 100
			8	0111 1000	Yul est 120
			8	1011 0100	Xlr est 180
			8	1101 0010	Ylr est 210
	Pzoi[3]	Mzoi[3]	1	0	Le segment verrouillé en octets ne suit pas
			1	1	Les zones spécifiées ne sont pas influencées par la méthode de protection
			1	0	Un item unique est spécifié
			2	11	Mode maximal
			2	00	Izoi utilise 8 bits pour un entier
			1	0	Izoi est décrit dans une seule dimension
		Izoi[3]	8	0000 0010	Les niveaux de résolution $\leq$ 2 sont spécifiés. (c'est-à-dire que les niveaux de résolution > 3 sont spécifiés avec mode maximal et commutation sur le complément.)
	Pzoi[4]	Mzoi[4]	1	0	Le segment verrouillé en octets ne suit pas
			1	0	Les zones spécifiées sont influencées par la méthode de protection
			1	0	Un item unique est spécifié
			2	11	Mode maximal
			2	00	Izoi utilise 8 bits pour un entier
			1	0	Izoi est décrit dans une seule dimension
		Izoi[4]	8	0000 0101	Les couches $\leq$ 5 sont spécifiées avec mode maximal.

Tableau B.7 – Description du modèle de déchiffrement dans le cas de l'algorithme AES-192/CBC

Paramètre				Longueur (bits)	Valeur	Signification déduite
P_{PM}	ME_{decry}			8	0000 0000	NULL: aucune méthode de prévention d'émulation de marqueur.
	CT_{decry}			16	0x0003	Identificateur de chiffrement: AES (chiffrement par blocs).
	CP_{decry}	M_{bc}		6	10 0000	Mode de chiffrement: CBC.
		P_{bc}		2	01	Mode de bourrage (bourrage PKCS#7).
		SIZ_{bs}		8	0001 0000	Longueur de bloc: 16 octets (128 bits)
		KT_{bc}	LK_{KT}	16	0x00C0	Longueur de clé: 192 bits
			KID_{KT}	8	0000 0011	Les informations sur les clés sont un identificateur URI
			LKI_{KT}	16	0x0021 (=33)	Longueur de l'identificateur URI: 33 octets.
			KI_{KT}	264	https://serveur/path/secretkey.pem	Cet identificateur URI est une adresse URL en protocole https; il doit être interprété par l'application au moyen de la syntaxe JPSEC. L'extraction effective de la clé est au-delà de la norme.

Tableau B.7 – Description du modèle de déchiffrement dans le cas de l'algorithme AES-192/CBC

Paramètre					Longueur (bits)	Valeur	Signification déduite
			G_{KT}	PO	16	0 000 001 010 011 100	Ordre de traitement: TRLCP.
				GV	8	0000 1001	Granularité de clé = aire totale dans la zone ZOI.
			V_{KT}	Nv	16	0x0001	Valeur de clé unique dans le paramètre KI_{KT}; valeurs non spécifiées dans VKT.
				Sv	16	0010 0001	Longueur de l'identificateur URI: 33 octets.
				VL	264	https://serveur/path/secretkey.pem	Cet identificateur URI est une localisation URL en protocole https; il doit être interprété par l'application au moyen de la syntaxe JPSEC. L'extraction effective de la clé est au-delà de la norme.

Tableau B.8 – Syntaxe du domaine de traitement

Paramètre	Longueur (bits)	Valeur	Signification déduite
PD	1	0_b	Le segment verrouillé en octets ne suit pas
	1	0_b	Hors du domaine des pixels
	1	0_b	Hors du domaine des coefficients d'ondelette
	1	0_b	Hors du domaine des coefficients d'ondelette quantifiés
	1	1_b	Traité dans le domaine du flux codé
	3	000_b	Non utilisé

Tableau B.9 – Syntaxe de la granularité et de la liste de valeurs

Paramètre		Longueur (bits)	Valeur	Signification déduite
G	PO	16	0 000 001 010 011 100	Ordre de traitement: TRLCP
	GV	8	0000 0110	L'unité de protection est le paquet
V	N_V	16	1	Le nombre de valeurs de vecteur d'initialisation est spécifié
	Sv	8	16	Longueur en octets du vecteur d'initialisation
	VL	128	*Valeur*	Valeur du vecteur d'initialisation

B.4.3 Conclusion

La technique présentée dans le présent article démontre le chiffrement sélectif pour les images JPEG 2000. Elle est fondée sur un chiffrement au niveau des paquets et sur des algorithmes de chiffrement normalisés et robustes. Elle peut être signalée au moyen des modèles définis dans le § 5.8. Elle prend en charge divers niveaux de complexité.

B.5 Outil de chiffrement pour contrôle d'accès JPEG 2000

B.5.1 Services de sécurité visés

Cette technologie fournit un outil de chiffrement qui peut empêcher l'émulation de marqueur dans un flux codé par chiffrement.

B.5.2 Applications typiques

Cette technologie permet un chiffrement sélectif et complet de flux à codage JPEG 2000. De telles méthodes de chiffrement sélectif peuvent servir à afficher seulement une image agréée, comme une vignette, une image de basse qualité et une image partiellement brouillée.

B.5.3 Utilisateurs potentiels, modèle d'implémentation et motivations

Fondamentalement, cette technologie est fondée sur un chiffrement en mode paquet d'un flux à codage JPEG 2000 avec un algorithme de chiffrement bien connu. Spécifiquement, cette technologie empêche l'émulation de marqueur dans le flux codé par chiffrement. Donc, même si le flux codé résultant du chiffrement est injecté dans un décodeur compatible avec la Partie 1 de la norme JPEG 2000, ce décodeur n'est pas susceptible de tomber en panne et peut reproduire correctement l'image protégée.

B.5.4 Aperçu technique

(1) Chiffrement

Etape 1 2 (octets) de code sont temporairement chiffrés au moyen d'un algorithme de chiffrement connu.

Etape 2 Si le code chiffré temporairement ou son code associé est supérieur à 0xFF8F, alors les 2 (octets) de code ne sont pas chiffrés.

Sinon, le code chiffré temporairement est extrait en tant que code chiffré.

Etape 3 On passe aux 2 (octets) de code suivants et les étapes 1 et 2 sont reprises.

Les 2 (octets) de code contenus dans le texte non chiffré doivent être inférieurs à 0xFF90 conformément à la spécification de la Partie 1. Par ailleurs, si le code chiffré temporairement ou son code associé est supérieur à 0xFF8F, alors les 2 (octets) de code ne sont pas chiffrés. En conséquence, les 2 (octets) de code contenus dans le cryptogramme sont inférieurs à 0xFF90.

Si la longueur du texte non chiffré a une valeur impaire, une exception au traitement est nécessaire; le dernier octet n'est pas chiffré ou justifié par bourrage avec un octet supplémentaire.

(2) Déchiffrement

Etape 1 2 (octets) de code sont temporairement déchiffrés au moyen du même algorithme cryptographique que lors du chiffrement.

Etape 2 Si le code déchiffré temporairement ou son code associé est supérieur à 0xFF8F, alors les 2 (octets) de code ne sont pas déchiffrés. Sinon, le code déchiffré temporairement est extrait en tant que code déchiffré.

Etape 3 On passe aux 2 (octets) de code suivants et les étapes 1 et 2 sont reprises.

Les 2 (octets) de code contenus dans le texte non chiffré original avant son chiffrement doivent être inférieurs à 0xFF90. Il est donc possible de tirer la conclusion que les 2 (octets) de code ne sont pas chiffrés si le code temporel déchiffré ou son code associé est supérieur à 0xFF8F.

B.5.5 Méthode de signalisation

Le Tableau B.10 montre des exemples de paramètres pour cette technologie. Tous les éventuels paramètres pour cette technologie doivent être signalés conformément à la syntaxe indiquée dans la norme JPSEC. En particulier, cette technologie devrait utiliser le modèle de "déchiffrement", la granularité de "paquet" et le domaine de traitement par "flux binaire" avec la zone ZOI appropriée.

Tableau B.10 – Exemples de paramètres pour cette technologie

Paramètre		Longueur (bits)	Valeur	Signification
SEC		16	0xFF65	Marqueur SEC
L_{SEC}		16	Variable	Longueur de segment marqueur SEC
Z_{SEC}		8	1 (exemple)	Indice de ce segment marqueur SEC
P_{SEC}		1	0	Un octet de segment FBAS ne suit pas
	F_{INSEC}	1	1 (exemple)	INSEC est utilisé
	$F_{multiSEC}$	1	0_b	Un seul segment marqueur SEC est utilisé
	F_{mod}	1	1_b	Des données originales JPEG 2000 ont été modifiées
	F_{TRLCP}	1	0_b	L'usage de balise indicielle TRLCP n'est pas défini
	Padding	3	000_b	Inutilisé
	N_{tools}	8 (RBAS)	1	Nombre d'outils de sécurité égal à 1
	I_{max}	8 (RBAS)	0	Indice maximal d'instance d'outil égal à 0
t		8 (FBAS)	1	Outil de protection JPSEC non normatif de l'organisme RA
i		8 (RBAS)	0000000_b	Indice d'instance d'outil
ID_{RA}	$ID_{RA,id}$	32	0	Identificateurs enregistrés
	$ID_{RA,nsl}$	8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$	168	*espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
L_{zoi}		16	9	La longueur de zone ZOI est 9 octets
ZOI		Variable	Voir Tableau B.11 (exemple)	Zone d'influence pour cet outil
L_{PID}		16	Variable	Longueur de L + T + PD + G
P_{ID}		Variable	Voir Tableau B.12 (exemple)	Paramètres pour cette technologie

Tableau B.11 – Exemple de zone ZOI de cet outil de production de clés

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NDzoi			8	1	Nombre de zones égal à 1
$Zone^0$	Dczoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	101000_b	Régions d'image et niveaux de résolution spécifiés dans l'ordre
	$Pzoi^1$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par la méthode de protection
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	1_b	Izoi est décrit dans deux dimensions
		$Izoi^1$	8	$0110\ 0100_b$	Xul est 100
			8	$0111\ 1000_b$	Yul est 120
			8	$1011\ 0100_b$	Xlr est 180
			8	$1101\ 0010_b$	Ylr est 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Les zones spécifiées ne sont pas influencées par la méthode de protection
			1	0_b	Un item unique est spécifié
			2	11_b	Mode maximal
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^3$	8	$0000\ 0010_b$	Des niveaux de résolution > 3 sont spécifiés.

Tableau B.12 – Identificateur P_{ID} pour cette technologie

Paramètre		Longueur (bits)	Valeur	Signification
T		Variable	Voir Tableau B.13	Modèles de déchiffrement
PD		8	$0000\ 1000_b$	Un octet de segment FBAS ne suit pas. Traité dans le domaine du flux codé
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100\ 0_b$	Ordre de traitement: pavé-résolution-couche-composante-district (TRLCP)
	GL	8	$0000\ 0110_b$	L'unité de protection est le paquet
Skip		8	0	*Sauter* le paramètre pour cet outil

Tableau B.13 – Exemple de modèle de déchiffrement de cette technologie

Paramètre		Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
ME_{decry}		8	1	Emulation de marqueur non intervenue
CT_{decry}		16	1	Chiffrement par blocs (AES)
CP_{decry}	M_{bc}	6	$10\ 0010_b$	Le mode OFB est utilisé. (Bits non justifiés par bourrage.)
	SIZ_{bc}	16	128	Longueur de bloc (128 bits)
	KT_{bc}	Variable	*Valeurs du modèle de clé*	Modèle de clé
	IVsc	128	*Valeur du vecteur d'initialisation*	Valeur du vecteur d'initialisation

B.5.6 Conclusion

Le présent paragraphe décrit une technologie de chiffrement pour un flux à codage JPEG 2000. L'avantage significatif de cette technologie doit empêcher l'émulation de marqueur d'intervenir dans le flux codé par chiffrement.

B.6 Outil de production de clés pour contrôle d'accès JPEG 2000

B.6.1 Services de sécurité visés

Cette technologie fournit un contrôle d'accès associé à l'image pour le système JPEG 2000 conformément à une structure hiérarchique dans ce système.

B.6.2 Applications typiques

Une application typique de cette technologie consiste à sécuriser la distribution d'images lorsque seul un utilisateur autorisé peut reproduire l'image acceptée. Par exemple, on est libre d'afficher une vignette, mais une image de grande résolution ne peut être décodée que par l'utilisateur qui en possède la clé.

B.6.3 Utilisateurs potentiels, modèle d'implémentation et motivations

Cette technologie prend en charge la production de clés à utiliser lors d'une distribution sécurisée d'images JPEG 2000. Cette technologie est fondée sur un contrôle d'accès associé à l'image, tel que région d'image, résolution et qualité d'image. Le principe de cette technologie consiste à produire le chiffrement et les clés de déchiffrement hiérarchiquement, au moyen d'une fonction de condensation cryptographique à sens unique telle qu'une fonction de hachage.

B.6.4 Aperçu technique

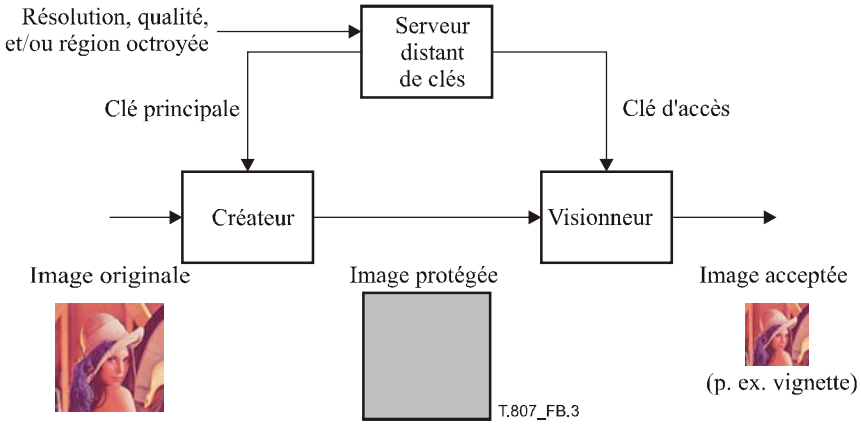


Figure B.3 – Aperçu général de cette technologie

Dans l'étape de chiffrement, un serveur distant de clés produit une clé principale. Puis un créateur chiffre une image au moyen de clés de paquet qui sont produites à partir de la clé principale. Au cours de l'étape de déchiffrement, un serveur distant de clés produit une clé d'accès conformément à une résolution, qualité, et/ou région octroyée. Puis un visionneur décrypte l'image chiffrée au moyen de clés de paquet produites à partir de la clé d'accès. Noter que ces clés sont produites séquentiellement sur la base d'une chaîne de hachage sécurisée.

Spécifiquement, cette technologie utilise la politique de contrôle d'accès suivante: "si un utilisateur peut accéder à un niveau de résolution ou à une couche, alors cet utilisateur peut également accéder aux niveaux inférieurs de cette résolution ou de cette couche". D'autre part, même si un utilisateur peut accéder à un pavé, il peut ne pas avoir accès du tout aux autres pavés.

L'avantage significatif de cette technologie est que le nombre de clés requises afin de passer d'un serveur distant de clés à un visionneur est très inférieur au cas conventionnel. Cela signifie que cette technologie permet de minimiser le surdébit en termes d'usage de capacité mémoire.

B.6.5 Méthode de signalisation

Le Tableau B.14 montre les paramètres recommandés dans cette technologie. Tous les éventuels paramètres doivent être signalés conformément à la syntaxe qui est identifiée dans le modèle JPSEC. Particulièrement, cet outil devrait utiliser le modèle de "déchiffrement", la granularité de "paquet" et le domaine de traitement de "flux binaire" avec la zone ZOI appropriée.

Tableau B.14 – Paramètres recommandés dans cette technologie

Paramètre		Longueur (bits)	Valeurs	Signification
SEC		16	0xFF65	Marqueur SEC
L_{SEC}		16	0 ... 255	Longueur de segment marqueur SEC
Z_{SEC}		8	0	Indice de ce segment marqueur SEC
P_{SEC}		1	0	Un octet de segment FBAS ne suit pas
	F_{INSEC}	1	1	INSEC est utilisé
	$F_{multiSEC}$	1	0_b	Un seul segment marqueur SEC est utilisé
	F_{mod}	1	1_b	Des données originales JPEG 2000 ont été modifiées
	F_{TRLCP}	1	0_b	L'usage de balise indicielle TRLCP n'est pas défini
	Padding	3	000_b	Inutilisé
	N_{tools}	8 (RBAS)	1	Nombre d'outils de sécurité égal à 1
	I_{max}	8 (RBAS)	0	Indice maximal d'instance d'outil égal à 0
t		8 (RBAS)	1	Outil JPSEC non normatif
i		8 (RBAS)	0	Indice d'instance pour cet outil
ID_{RA}	$ID_{RA,id}$	32	5	Identificateurs enregistrés pour cet outil
	$ID_{RA,nsl}$	8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$	168	*espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
L_{zoi}		16	Variable	Longueur de zone ZOI pour cet outil
ZOI		Variable	*Valeur ZOI*	Zone d'influence pour cet outil
L_{PID}		16	Variable	Longueur de L + T + PD + G
P_{ID}		Variable	Voir Tableau B.16	Paramètres pour cette technologie

Tableau B.15 – Exemple de zone ZOI de cet outil de production de clés

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NDzoi			8	1	Nombre de zone égal à 1
$Zone^0$	Dczoi		1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Classe de description associée à l'image
			6	101000_b	Régions d'image et niveaux de résolution spécifiés dans l'ordre
	$Pzoi^1$	$Mzoi^1$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	0_b	Les zones spécifiées sont influencées par la méthode de protection
			1	0_b	Un item unique est spécifié
			2	00_b	Mode rectangulaire
			2	00_b	Izoi utilise 8 bits pour un entier
			1	1_b	Izoi est décrit dans deux dimensions
		$Izoi^1$	8	$0110\ 0100_b$	Xul est 100
			8	$0111\ 1000_b$	Yul est 120
			8	$1011\ 0100_b$	Xlr est 180
			8	$1101\ 0010_b$	Ylr est 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	Le segment verrouillé en octets ne suit pas
			1	1_b	Les zones spécifiées ne sont pas influencées par la méthode de protection
			1	0_b	Un item unique est spécifié
			2	11_b	Mode maximal
			2	00_b	Izoi utilise 8 bits pour un entier
			1	0_b	Izoi est décrit dans une seule dimension
		$Izoi^3$	8	$0000\ 0010_b$	Les niveaux de résolution > 3 sont spécifiés.

Tableau B.16 – Identificateur P_{ID} pour cette technologie

Paramètre		Longueur (bits)	Valeurs	Signification
T		Variable	Voir Tableau B.17	Modèles de déchiffrement
PD		8	$0000\ 1000_b$	Un octet de segment FBAS ne suit pas. Traité dans le domaine du flux codé.
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Ordre de traitement: pavé-résolution-couche-composante-district.
	GL	8	$0000\ 0110_b$	L'unité de protection est le paquet
H		16	Voir Tableau 37 dans le § 5.8.3.1	Fonction de hachage pour cet outil de production de clés
L_k		8	0 ... 255	Longueur des informations d'accès aux clés
AK_{info}		Variable	*Accès clé valeur*	Informations sur les clés d'accès (ces informations sont chiffrées au moyen de KT_{bc} dans T).

Tableau B.17 – Exemple de modèle de déchiffrement de cette technologie

Paramètre		Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
ME_{decry}		8	1	Emulation de marqueur non intervenue
CT_{decry}		16	3	Chiffrement par blocs (AES)
CP_{decry}	M_{bc}	6	10 0010	Le mode OFB est utilisé. (Bits non justifiés par bourrage.)
	SIZ_{bc}	16	128	Longueur de bloc (128 bits)
	KT_{bc}	Variable	Voir § 5.8.5	Modèle de clé
	IVsc	128	*Valeur du vecteur d'initialisation*	Valeur du vecteur d'initialisation

B.6.6 Conclusion

Le présent paragraphe décrit une technologie de contrôle d'accès associé à l'image pour un flux à codage JPEG 2000. L'avantage significatif de cette technologie est que le nombre de clés à gérer et à extraire est très inférieur au cas conventionnel.

B.7 Brassage par ondelette et par domaine de flux binaire pour contrôle d'accès conditionnel

B.7.1 Résumé

Le contrôle d'accès à une image est une fonctionnalité importante en imagerie sécurisée. Il est souvent souhaitable de donner accès à une vignette de basse résolution ou à une image de basse qualité, tandis que l'accès à des résolutions ou qualités supérieures est soumis à autorisation. Dans le présent paragraphe, une technique de contrôle d'accès conditionnel est présentée. Cette méthode a été initialement présentée dans la référence [23]. Fondamentalement, elle ajoute un bruit pseudo-aléatoire à l'image. Les utilisateurs autorisés connaissent la séquence pseudo-aléatoire et peuvent donc supprimer ce bruit. Inversement, les utilisateurs non autorisés n'ont accès qu'à des images gravement distordues. Le système se compose de trois composants principaux: brassage, générateur de nombres pseudo-aléatoires et algorithme de chiffrement. Afin d'exploiter et de conserver complètement les propriétés du codage JPEG 2000, le brassage est appliqué sélectivement aux blocs de code composant le flux codé. Par conséquent, le niveau de distorsion introduit dans des parties spécifiques de l'image peut être contrôlé. Cela permet d'effectuer un contrôle d'accès par résolution, par qualité ou par région d'intérêt dans une image.

B.7.2 Aperçu technique

Le système se compose de trois composants principaux:

- brassage: deux méthodes sont prises en charge. Le brassage est effectué soit sur les coefficients quantifiés d'ondelette, ou directement sur les bits du flux codé. Dans le premier cas, les signes des coefficients contenus dans chaque bloc de code sont inversés pseudo-aléatoirement. Dans le second cas, les bits du flux codé sont inversés pseudo-aléatoirement;
- générateur de nombres pseudo-aléatoires (PRNG): le générateur PRNG sert à piloter le brassage. Il est fondé sur une valeur d'initialisation (germe). Dans une matérialisation préférée de cette technique, l'algorithme SHA1PRNG [24] est utilisé avec un germe de 64 bits dans le générateur de nombres pseudo-aléatoires (PRNG). Noter que d'autres algorithmes de générateur PRNG pourraient être utilisés également;
- algorithme de chiffrement: afin de les communiquer aux utilisateurs autorisés, les germes sont chiffrés et insérés dans le flux codé. Dans une matérialisation préférée de la technique, l'algorithme RSA est utilisé pour le chiffrement [25]. D'autres algorithmes de chiffrement pourraient être utilisés également. La longueur de la clé peut être sélectionnée au moment où l'image est protégée.

Les Figures B.4 et B.5 correspondent aux deux cas de brassage: dans le domaine des ondelettes et dans celui des flux binaires.

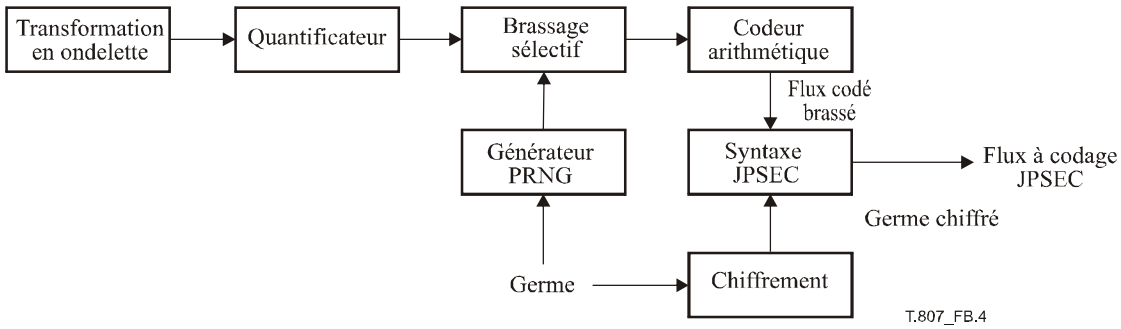


Figure B.4 – Schéma fonctionnel du brassage dans le domaine des ondelettes

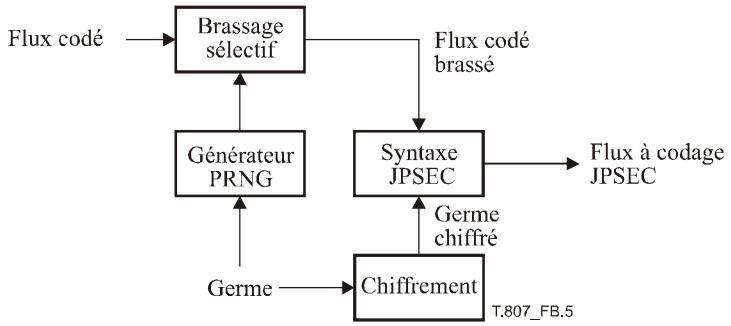


Figure B.5 – Schéma fonctionnel du brassage dans le domaine des flux binaires

Afin d'améliorer la sécurité du système, le germe peut être modifié d'un bloc de code à un autre. De même, plusieurs niveaux d'accès peuvent être définis, au moyen de différentes clés de chiffrement. La syntaxe indiquée ci-dessous est très flexible et prend en charge l'usage de multiples germes et clés.

B.7.3 Syntaxe du flux codé

Dans cet exemple, les deux segments marqueurs, SEC et INSEC, sont utilisés. La syntaxe du flux codé est définie ci-dessous. Le segment marqueur SEC utilise la syntaxe pour les outils non normatifs. Le segment marqueur INSEC sert à signaler quels blocs de code sont embrouillés et quels germes sont utilisés.

B.7.3.1 Syntaxe pour segment marqueur SEC

La syntaxe des outils non normatifs est utilisée. Dans le cas de clés multiples, plusieurs instances de l'outil sont utilisées dans le segment marqueur SEC. Plus spécifiquement, plusieurs instances i = 0, 1, 2, … ayant le même ID sont présentes, chacune correspondant à un identificateur de clé différent $KeyID^{(i)}$. Cette syntaxe est illustrée ci-dessous. Voir la Figure B.6.

t	i = 0	ID	$L_{ZOI}^{(0)}$	$ZOI^{(0)}$	$L_{PID}^{(0)}$	$N_S^{(0)}$	$KeyID^{(0)}$	Données
t	i = 1	ID	$L_{ZOI}^{(1)}$	$ZOI^{(1)}$	$L_{PID}^{(1)}$	$N_S^{(1)}$	$KeyID^{(1)}$	Données
t	i = 2	ID	$L_{ZOI}^{(2)}$	$ZOI^{(2)}$	$L_{PID}^{(2)}$	$N_S^{(2)}$	$KeyID^{(2)}$	Données

Figure B.6 – Syntaxe d'outil de protection non normatif dans le cas de clés multiples

Avec la sémantique suivante pour P_{ID}:

Tableau B.18 – Syntaxe et sémantique pour P_{ID}

Paramètres	Longueur (en bits)	Signification
N_s	16	Nombre de germes utilisés par cette instance
KeyID	32	Identification de la clé à utiliser pour le déchiffrement
Data	Variable	Germes chiffrés

B.7.3.2 Syntaxe pour le segment marqueur INSEC

Afin d'inclure les informations indiquant quel germe sert à protéger quels blocs de code, le marqueur du flux codé entrant (INSEC) est également utilisé. Dans cet exemple, il est ajouté avant le ou les blocs de code sécurisés, afin d'indiquer quel germe a servi à protéger ce ou ces blocs de code. Au lieu d'indiquer le germe proprement dit, le marqueur contient un indice qui se rapporte aux germes contenus dans le segment marqueur SEC de l'en-tête principal. Comme, dans cet exemple, les informations de marqueur INSEC s'appliquent aux blocs de code suivants, R est toujours égal à 1. La syntaxe de AP est différente dans le cas du brassage d'ondelette et dans celui du brassage de flux binaire:

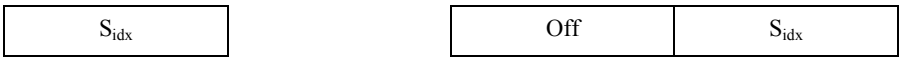


Figure B.7 – Syntaxe pour AP: brassage dans le domaine des ondelettes (à gauche); brassage dans le domaine des flux binaires (à droite)

Avec la sémantique suivante:

Tableau B.19 – Syntaxe et sémantique pour AP

Paramètre	Longueur (en bits)	Signification
Off	16	Décalage du premier octet brouillé dans le flux binaire du bloc codé
S_{idx}	16	Indice de germe pour le bloc de code

Dans le cas de clés multiples, la combinaison de l'instance d'outil i et de l'indice de germe S_{idx} identifie de façon unique à quel germe/quelle clé ce segment marqueur INSEC se rapporte actuellement.

B.7.4 Conclusions

Dans le présent paragraphe, un outil de sécurité a été présenté pour contrôle d'accès conditionnel à des images JPEG 2000. Cette technique introduit un bruit pseudo-aléatoire dans des parties sélectionnées du flux codé. Par conséquent, l'image décodée apparaît très distordue pour un décodeur non autorisé qui ne sait pas comment supprimer ce bruit.

La sécurité de la technique dépend de la sécurité des algorithmes spécifiques pour le générateur de nombres pseudo-aléatoires et pour le chiffrement du germe, dans nos matérialisations préférées, SHA1PRNG et RSA respectivement. SHA1PRNG est un générateur PRNG sécurisé, car aucune connaissance de la séquence ne peut être déduite de la connaissance de certains des nombres contenus dans la séquence. Dans cet exemple, le germe du générateur PRNG a une longueur de 64 bits, ce qui devrait rendre impossible une attaque exhaustive. Les germes sont chiffrés avec l'algorithme RSA au moyen d'une clé de longueur définie par l'utilisateur. L'algorithme RSA est considéré comme un algorithme sécurisé, à condition qu'une longueur de clé suffisante soit utilisée.

B.8 Accès progressif pour flux à codage JPEG 2000

B.8.1 Services de sécurité visés

Cette méthode fournit un contrôle d'accès non associé à l'image pour un flux à codage JPEG 2000 conformément à un ordre de progression d'un flux codé.

B.8.2 Application typiques

Une application typique de cette technologie est la sécurisation de la distribution d'image où seul un utilisateur autorisé peut reproduire l'image acceptée. Spécifiquement, cette technologie convient au contrôle d'accès conformément à un ordre de progression d'un flux codé.

B.8.3 Utilisateurs potentiels, modèle d'implémentation et motivations

Lors de la conception du procédé de contrôle d'accès, le défi consiste à trouver un équilibre délicat entre sécurité, efficacité et flexibilité. Cette technique de contrôle d'accès pour flux à codage JPEG 2000 construit une chaîne de hachage afin de produire les clés pour chaque paquet et ainsi chiffrer les paquets dans le flux codé. Seuls les utilisateurs possédant l'habilitation correcte de sécurité peuvent donc déchiffrer les paquets correspondant à l'image octroyée dans le flux codé.

B.8.4 Aperçu technique

Dans l'étape de chiffrement, un serveur distant de clés produit une clé principale. Puis un créateur chiffre un flux codé au moyen de clés de paquet qui sont produites à partir de la clé principale. Au cours de l'étape de déchiffrement, un serveur distant de clés produit une clé d'accès conformément au paquet octroyé. Puis un visionneur décrypte le flux codé par chiffrement au moyen des clés de paquet produites à partir de cette clé d'accès.

Spécifiquement, cette technologie utilise la politique de contrôle d'accès ci-après: "si un utilisateur peut accéder à un paquet, alors cet utilisateur peut également avoir accès aux paquets antécédents d'un flux codé". On appelle donc une telle sorte de contrôle d'accès "*accès progressif*".

L'avantage significatif de cette technologie est que le nombre de clés requises afin de passer d'un serveur distant de clés à un visionneur est très inférieur au cas conventionnel. Cela signifie que cette technologie permet de minimiser le surdébit en termes d'usage de capacité mémoire.

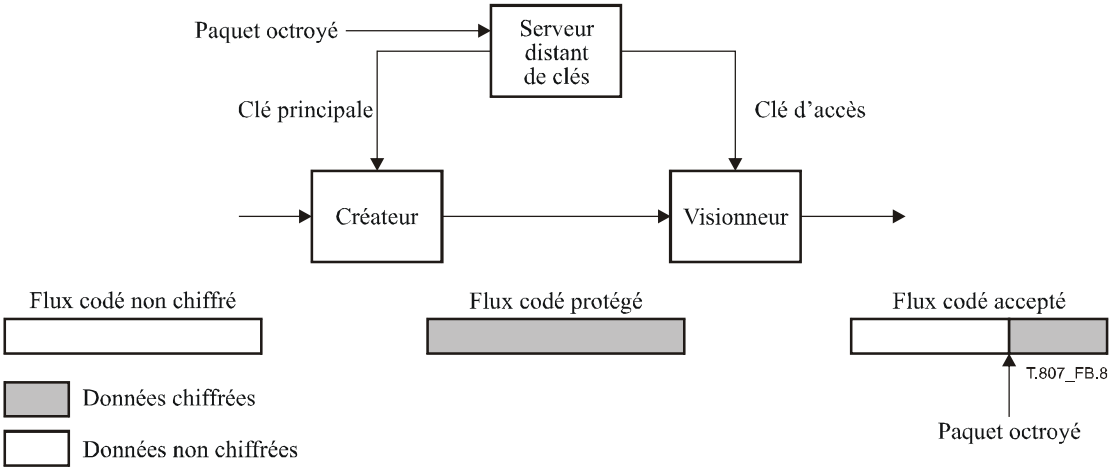


Figure B.8 – Aperçu technique de cette technologie

B.8.5 Méthode de signalisation

Le Tableau B.20 montre les paramètres recommandés dans cette technologie. Tous les éventuels paramètres doivent être signalés conformément à la syntaxe identifiée dans le modèle JPSEC. Particulièrement, cette technologie devrait utiliser le modèle de "déchiffrement", la granularité de "paquet" et le domaine de traitement de "flux binaire" avec la zone ZOI appropriée.

Tableau B.20 – Exemples de paramètres pour cet outil

Paramètre		Longueur (bits)	Valeurs	Signification
SEC		16	0xFF65	Marqueur SEC
L_{SEC}		16	Variable 0 ... 255	Longueur de segment marqueur SEC
Z_{SEC}		8	0	Indice de ce segment marqueur SEC
P_{SEC}		1	0	Un octet de segment FBAS ne suit pas
	F_{INSEC}	1	1_b	INSEC est utilisé
	$F_{multiSEC}$	1	0_b	Un seul segment marqueur SEC est utilisé
	F_{mod}	1	1_b	Des données originales JPEG 2000 ont été modifiées
	F_{TRLCP}	1	0_b	L'usage de balise indicielle TRLCP n'est pas défini
	Padding	3	000_b	Inutilisé
	N_{tools}	8 (RBAS)	1	Nombre d'outils de sécurité égal à 1
	I_{max}	8 (RBAS)	0	Indice maximal d'instance d'outil égal à 0
t		8 (RBAS)	1	Outil de protection RA
i		8 (RBAS)	0	Indice d'instance
ID_{RA}	$ID_{RA,id}$	32	7	Identificateurs enregistrés
	$ID_{RA,nsl}$	8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$	168	*espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
L_{zoi}		16 (RBAS)	Variable	Longueur de zone ZOI
ZOI		Variable	Voir Tableau B.21 (exemple)	Zone d'influence pour cet outil
L_{PID}		16 (RBAS)	Variable	Longueur de L + T + PD + G
P_{ID}		Variable	Voir Tableau B.22 (exemple)	Paramètres pour cet outil

Tableau B.21 – Exemple de zone ZOI de cette technologie

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
NDzoi			8	1	Nombre de zone égal à 1
$Zone^0$	DCzoi		1	0	Le segment verrouillé en octets ne suit pas
			1	1	Classe de description non associée à l'image
			6	000100	Des paquets sont spécifiés
	$Pzoi^4$	$Mzoi^4$	0	1	Le segment verrouillé en octets ne suit pas
			1	1	Les zones spécifiées ne sont pas influencées par la méthode de protection
			1	1	De multiples items sont spécifiés
			11	2	Mode maximal
			00	2	Izoi utilise 8 bits pour un entier
			00	2	Izoi est décrit dans une seule dimension
		$Izoi^{11}$	8	0000 1010	Un indice de paquet > 10 est identifié

Tableau B.22 – P_{ID} pour cette technologie

Paramètre		Longueur (bits)	Valeurs	Signification
T		Variable	Voir Tableau B.23	Modèles de déchiffrement
PD		8	$0000\ 1000_b$	Un octet subséquent de segment BAS n'existe pas. Domaine du flux codé.
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Ordre de traitement: pavé-résolution-couche-composante-district.
	GL	8	$0000\ 0110_b$	L'unité de protection est le paquet
H		16	Voir Tableau 38 dans le § 5.8.3.1	Fonction de hachage pour cet outil de production de clés
L_k		8	0 – 255	Longueur des informations d'accès aux clés
AK_{info}		Variable	*Valeur de clé d'accès*	Informations sur les clés d'accès (ces informations sont chiffrées au moyen de KT_{bc} dans T).

Tableau B.23 – Exemple de modèle de déchiffrement dans cette technologie

Paramètre		Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
ME_{decry}		8	1	Emulation de marqueur non intervenue
CT_{decry}		16	3	Chiffrement par blocs (AES)
CP_{decry}	M_{bc}	6	10 0010	Le mode OFB est utilisé. (Bits non justifiés par bourrage.)
	SIZ_{bc}	16	128	Longueur de bloc (128 bits)
	KT_{bc}	Variable	*Valeurs du modèle de clé*	Modèle de clé
	IVsc	128	*Valeur du vecteur d'initialisation*	Valeur du vecteur d'initialisation

B.8.6 Conclusion

Le présent paragraphe décrit une technologie de contrôle d'accès pour un flux à codage JPEG 2000. L'avantage significatif de cette technologie est que le nombre de clés à gérer et à extraire est très inférieur au cas conventionnel. Cette technologie fournit un contrôle d'accès JPEG 2000 flexible et efficace, conformément à une progression ordonnée dans un flux codé.

B.9 Authenticité modulable du flux à codage JPEG 2000

B.9.1 Service de sécurité

Le présent paragraphe fournit un mécanisme d'authentification flexible pour des flux à codage JPEG 2000. Il permet aux utilisateurs de vérifier l'authenticité et l'intégrité de différentes sous-images avec une unique signature numérique.

B.9.2 Application typique

Dans des domaines d'application critiques tels qu'administrations publiques, finances, médecine et droit, les clients exigent normalement l'authenticité du contenu reçu. En conséquence, un mécanisme de sécurité modulable d'authentification des documents est requis lors de la dissémination de contenus.

B.9.3 Motivation

Dans les applications de publication par tierce partie, un producteur d'images engendre un flux codé et sa signature. Le producteur achemine ensuite le flux codé et la signature à un éditeur tiers. Les utilisateurs peuvent demander à l'éditeur un flux transcodé en raison d'une limitation des ressources (p. ex. en termes de largeur de bande ou de puissance de calcul). L'éditeur acheminera alors vers l'utilisateur les sous-données d'image ainsi que leur preuve d'authenticité.

B.9.4 Aperçu technique

Le procédé fournit un mécanisme d'authentification flexible pour des flux à codage JPEG 2000. Il contient trois modules: signature, transcodage et vérification. La technologie de base est l'arborescence Merkle, qui organise les paquets JPEG 2000.

B.9.4.1 Module de signature

Le module de signature produit une signature à une entrée de flux à codage JPEG 2000 conformément à un procédé préféré de signature numérique. Le flux codé et protégé est produit par insertion d'un marqueur SEC dans le flux codé original. Spécifiquement, le producteur:

- lit un flux à codage JPEG 2000;
- construit un arbre de hachage afin de produire la valeur *racine*. La valeur de chaque nœud folié est le hachage d'un paquet. La valeur de chaque nœud interne est le hachage de ses nœuds descendants. La structure arborescente est similaire à l'ordre de progression du flux codé;
- signe la valeur *racine* de l'arbre de hachage avec une clé privée fondée sur un algorithme de signature;
- crée les paramètres SEC et les insère dans le segment marqueur SEC afin de produire un authentique flux codé.

B.9.4.2 Module de transcodage

Ce module produit des jetons d'intégrité subsidiaires (SIT, *subsidiary integrity token*) et un flux transcodé fondé sur la résolution, la couche, la composante et la région demandées. Le marqueur SEC du nouveau flux codé contient les jetons SIT et certains autres paramètres. Spécifiquement, l'éditeur et/ou le serveur intermédiaire:

- lisent les paquets rejetés qui ne sont pas inclus dans le flux transcodé;
- construisent les sous-arbres de hachage avec les paquets rejetés;
- insèrent les valeurs radicales des sous-arbres dans le segment marqueur SEC.

Le flux transcodé contient le segment marqueur SEC mis à jour et le flux codé mis à jour, à l'exclusion des paquets rejetés.

B.9.4.3 Module de vérification

Le module de vérification vérifie l'authenticité du flux codé protégé. Conformément au procédé préféré de signature numérique, le vérificateur obtient la clé publique, puis:

- lit le flux codé reçu;
- construit l'arbre de hachage de bas en haut avec les paquets et les en-têtes de flux codé reçus. Si certains paquets sont rejetés, remplacer le sous-arbre par le jeton SIT correspondant. Puis la valeur *racine* est construite;
- vérifie la valeur *racine* en fonction de la signature contenue dans le segment marqueur SEC et fondée sur le système de signature particulier. En cas de concordance, le flux codé est accepté; sinon les paquets reçus sont rejetés.

B.9.5 Syntaxe du flux codé

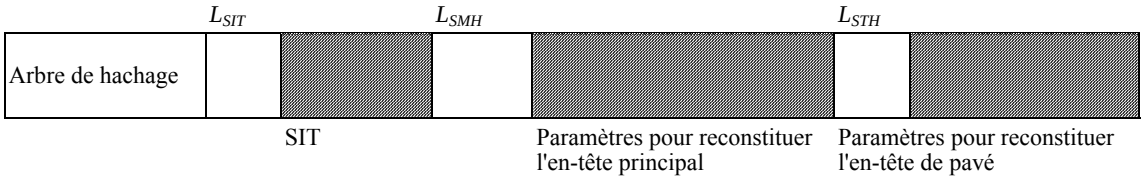
La structure de marqueur SEC est représentée dans le Tableau B.24, qui contient le marqueur SEC, l'identificateur d'outil, la zone ZOI, le modèle d'authentification et les paramètres de sécurité pour vérification. Les paramètres de sécurité comprennent les données permettant de reconstituer les en-têtes du flux codé.

Tableau B.24 – Syntaxe d'outil non normatif

t	i	ID	L_{ZOI}	ZoI_{ID}	L_{ID}	PM_{ID}	T	TP_{ID}

Paramètre		Longueur (bits)	Valeurs	Sémantique
t		8 (RBAS)	1	Outil de protection de l'organisme d'enregistrement
i		8 (RBAS)	*Valeur d'instance*	Identificateur d'instance d'outil
ID_{RA}	$ID_{RA,id}$	32	*Valeur d'identificateur*	Identificateurs enregistrés
	$ID_{RA,nsl}$	8 (RBAS)	21	Longueur de $ID_{RA,ns}$ en octets
	$ID_{RA,ns}$	168	*espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
L_{ZOI}		16	$[0 \ldots 2^{16} - 1]$	Longueur des paramètres pour ZOI
ZOI_{ID}		Variable	Valeurs ZOI	Paramètres de zone
L_{ID}		16	$[19 \ldots 2^{16} - 1]$	Longueur des paramètres
ID_T		8	2	Identificateur de classe de modèle d'authentification
T		Variable	*Valeurs du modèle d'authentification*	Modèle d'authentification/de code MAC
TP_{ID}		Variable	Voir Tableau B.25	Paramètres de sécurité

Tableau B.25 – Paramètres de sécurité



Paramètre	Longueur (bits)	Valeurs	Signification
Arbre de hachage	8	0 ... (2^8 – 1)	Ordre hiérarchique de hachage, qui peut être différent de l'ordre de progression du flux codé. Provisoirement: 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL autres: réservé
L_{SIT}	16	0 ... (2^{16} – 1)	Nombre de jetons SIT
SIT	Variable: L_{hash}*L_{SIT}	NaN	Jeton d'intégrité subsidiaire (SIT)
L_{SMH}	16	0 ... (2^{16} – 1)	Longueur pour SMH
SMH	Variable		Parameters for recovering main header
L_{STH}	16	0 ... (2^{16} – 1)	Longueur pour STH
STH	Variable		Paramètres pour reconstituer en-tête de pavé
a) Pour l'authentification par code MAC à clés calculées, la clé (de vérification) devrait être remise séparément. b) NaN: valeur non numérique. c) L_{hash} longueur de la valeur de hachage, p. ex., 160 pour l'algorithme SHA1.			

B.9.6 Conclusion

Cette technologie fournit un mécanisme d'authentification flexible pour des flux à codage JPEG 2000. Elle possède la propriété de "signer une fois et vérifier de nombreuses façons". Concrètement, une fois qu'un flux à codage JPEG 2000 original est signé, divers flux transcodés à partir du flux codé original peuvent être vérifiés en ne faisant confiance qu'au producteur. Cette propriété correspond parfaitement à la fonctionnalité de "comprimer une fois et décomprimer de nombreuses façons". Elle s'oppose à la méthode traditionnelle d'authentification des images qui permet à une seule signature de n'authentifier qu'une seule image.

B.10 Confidentialité des données JPEG 2000 et système de contrôle d'accès fondé sur le découpage et le masquage de données

Le système décrit dans le présent paragraphe est fondé sur le découpage, au moyen d'un processus appelé *découpage_et_masquage_des_données*, d'un fichier JPEG 2000 original en deux nouveaux fichiers appelés respectivement *Fichier_jp2_masqué* qui achemine un contenu protégé et *Fichier_de_commande* qui achemine les informations nécessaires à l'accès au contenu protégé. Seule une combinaison en temps réel de ces deux fichiers, au moyen du processus intitulé *Composition_directe*, permet de reconstruire le fichier JPEG 2000 original. Le processus de Composition_directe est régi par des règles de contrôle d'accès et par une gestion des droits. Le système décrit fournit un haut niveau de robustesse et de flexibilité en termes de confidentialité des données JPEG 2000 et de contrôle d'accès. Il est fondé sur des opérations mathématiques à faible consommation de temps et de ressources financières.

B.10.1 Description opérationnelle

B.10.1.1 Services de sécurité visés

– Confidentialité: un Fichier_jp2_masqué achemine un contenu protégé. Par simple décodage d'un unique Fichier_jp2_masqué, le contenu restitué est visuellement brouillé, empêchant donc d'accéder au contenu original. Seule la reconstitution en temps réel des données mémorisées dans le Fichier_de_commande au moyen du processus de Composition_directe permet d'accéder au contenu original.

– Contrôle d'accès: ce système peut servir à exécuter un contrôle d'accès sur un contenu d'image: plusieurs utilisateurs se partageant le même Fichier_jp2_masqué mais possédant différents droits d'accès ne seront pas autorisés à accéder aux mêmes parties du contenu.

Note sur la protection des droits IPR: en associant l'accès au contenu à l'authentification et à la gestion des droits, une commande et un suivi efficaces de la diffusion et de l'usage d'un contenu protégé peuvent être garantis conformément à la volonté et à la prérogative de son propriétaire, éventuellement par combinaison de ce système avec un filigranage ou la prise d'empreintes digitales.

B.10.1.2 Application typiques

Un des traits fondamentaux du système décrit est le découpage du flux JPEG 2000 initial en deux fichiers: le premier (Fichier_jp2_masqué) acheminant seulement 99% des données originales et 1% de données fictives appelées *leurres* et pouvant être librement distribué, diffusé, échangé ou copié au moyen de tout réseau ou média classique; et le second (Fichier_de_commande) acheminant 1% des données originales plus certaines informations, les unes et les autres étant absolument nécessaires afin d'accéder au contenu protégé qui est acheminé dans le Fichier_jp2_masqué.

L'autre trait fondamental consiste à associer l'accès au contenu protégé qui est acheminé dans le Fichier_jp2_masqué à une identification et à des étapes de gestion des droits dont les résultats vont déclencher le flux direct des informations requises afin de reconstituer – en temps réel seulement – un contenu désembrouillé.

Finalement, un suivi et un compte rendu efficaces de l'utilisation sont activés au moyen des statistiques collectées à partir des fichiers de journalisation sécurisés du serveur distant des fichiers_de_commande.

B.10.1.3 Utilisateurs potentiels, modèle d'implémentation et motivations

Les utilisateurs potentiels du système décrit sont les créateurs, les propriétaires et les fournisseurs de contenu car le système garantit qu'une fois le contenu protégé et acheminé dans un Fichier_jp2_masqué, seuls les utilisateurs authentifiés et autorisés seront en mesure d'accéder au contenu original. Il est important de mettre en évidence le fait que 99% seulement du contenu original est fourni librement, tandis que le centième nécessaire afin d'accéder au contenu original ne sera distribué qu'après exécution des protocoles d'authentification et de gestion des droits.

B.10.2 Aperçu technique

La Figure B.9 montre un aperçu général du système.

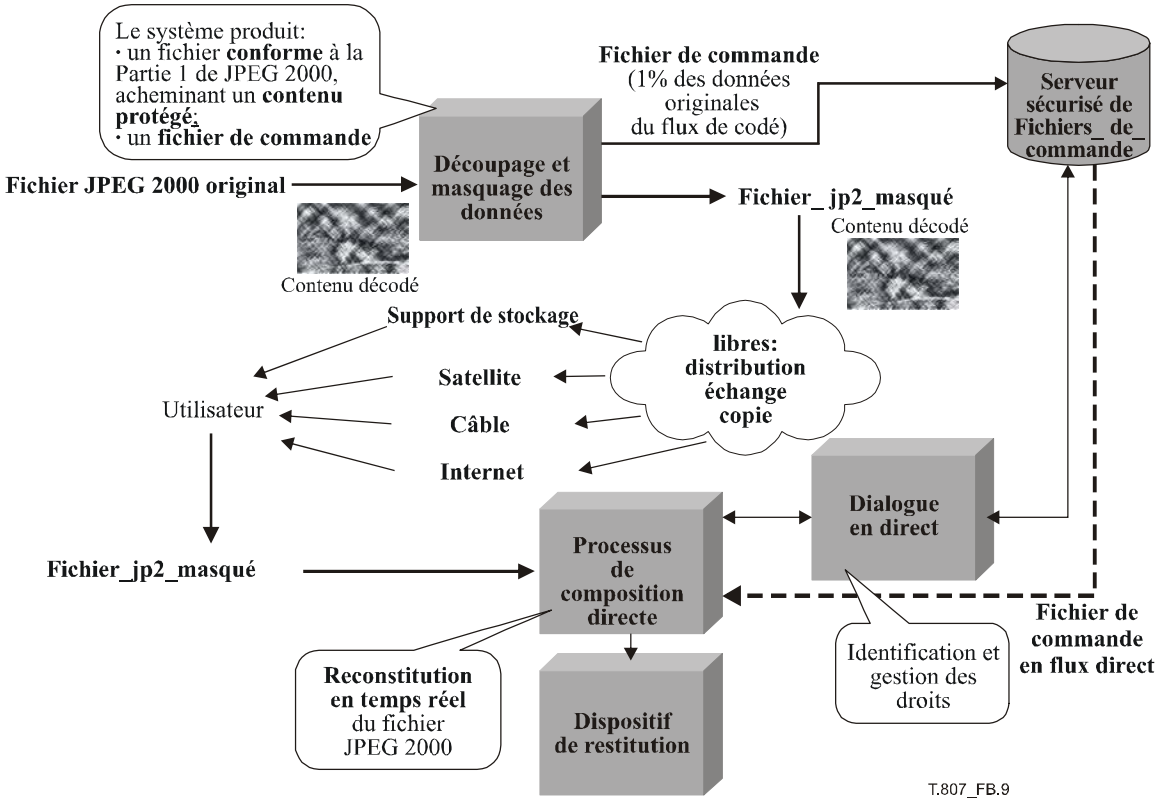


Figure B.9 – Aperçu général du système

Un fichier d'entrée JPEG 2000 est découpé en deux nouveaux fichiers au moyen d'une opération appelée *découpage et masquage de données*. Deux nouveaux fichiers sont alors produits: un *Fichier_jp2_masqué*, acheminant un contenu protégé (contenu JPSEC) et un *Fichier_de_commande*.

Au moyen du processus de découpage et de masquage des données, certaines portions du fichier JPEG 2000 original sont extraites et remplacées par des leurres. Un Fichier_jp2_masqué achemine à peu près 99% du contenu original tandis que le dernier centième contient des données fictives appelées *leurres*, c'est-à-dire des données sans aucune liaison préalablement connue avec les données originales. Contrairement au chiffrement classique, le processus de masquage n'est pas fondé sur des clés. Un Fichier_jp2_masqué peut être librement distribué, échangé ou copié par tout utilisateur. Le Fichier_de_commande contient le centième des données originales extraites du fichier original. Il est mémorisé dans un *Serveur sécurisé de Fichiers_de_commande*.

Quand le Fichier_jp2_masqué est décodé par un décodeur conforme à la Partie 1 de la norme JPEG 2000, le contenu apparaît visuellement brouillé. Le seul moyen d'accéder au contenu original consiste à reconstituer les données originales extraites grâce au Fichier_de_commande. Le dispositif de *Composition_directe* se connecte au serveur sécurisé de Fichiers_de_commande au moyen du protocole intitulé *Dialogue_en_direct*, puis un protocole d'identification et de gestion des droits se déroule comme suit:

- si l'utilisateur possède les droits ou accepte les conditions d'accès au contenu (p. ex. paiement ou abonnement), les données récupérées sont extraites du Fichier_de_commande et le fichier JPEG 2000 original est récupéré en temps réel. Cependant, conformément aux droits de l'utilisateur, la reconstitution du contenu JPEG 2000 original peut être partielle (par exemple afin de permettre d'accéder seulement à un certain pavé et/ou composante chromatique et/ou résolution et/ou district et/ou couches qualitatives) ou être complète;
- si l'utilisateur ne possède pas les droits ou n'accepte pas les conditions, seul le contenu brouillé est affiché.

Les principales caractéristiques du système décrit sont les suivantes:

- *découpage du fichier JPEG 2000 original* en deux fichiers, le premier acheminant un contenu JPEG 2000 protégé avec seulement 99% des données originales plus 1% de données fictives appelées *leurres* (Fichier_jp2_masqué), le second mémorisant certaines données informatives originales (1%) qui sont requises afin de reconstruire le contenu original JPEG 2000;
- *brassage visuel* du contenu;
- conformité à la Partie 1 de la norme JPEG 2000 et *préservation de la longueur du fichier*;
- système de protection *à bas débit binaire et à faible coût de calcul*.

Le système décrit peut être utilisé avec tout environnement et/ou système d'exploitation. Aucune exigence particulière n'est prescrite concernant le matériel ou le logiciel.

Le processus de masquage va insérer le marqueur SEC suivant dans le Fichier_jp2_masqué:

Tableau B.26 – Valeurs paramétriques pour cet outil

Paramètre		Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
SEC		16	0xFF65	Marqueur SEC
L_{SEC}		16	0xXXXX	Longueur du segment marqueur SEC
Z_{SEC}		8	1-255	Indice du segment marqueur
P_{SEC} (si $Z_{SEC} = 1$)	F_{INSEC}	1	0	INSEC n'est pas utilisé
	$F_{multiSEC}$	1	0	Un seul segment marqueur SEC est utilisé
	F_{J2K}	2	1	Flux JPSEC conforme à la Partie 1 de la norme JPEG 2000
	F_{TRLCP}	1	0	L'usage de balise indicielle TRLCP n'est pas défini dans ce champ.
	N_{tools}	7	1	Un seul outil de sécurité est utilisé dans le flux codé
	I_{max}	7	1	Valeur maximale d'indice d'instance de l'outil utilisé
	Padding	5	0	Bourrage

Tableau B.26 – Valeurs paramétriques pour cet outil

Paramètre					Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
$Tool^{(0)}$	t				8 (RBAS)	1	Outil de protection non normatif
	i				8 (RBAS)	0	Indice d'instance d'outil
	ID_{RA}	$ID_{RA,id}$			32	ID	RA sert à fournir le numéro d'identification
		$ID_{RA,nsl}$			8 (RBAS)	21	Longueur de $ID_{RA,ns}$: 21 octets.
		$ID_{RA,ns}$			168	*Espace nominatif*	Espace nominatif de l'organisme RA auprès duquel cet outil est enregistré
	L_{ZOI}				16	*Valeur de longueur*	Longueur de L_{ZOI} + ZOI
	ZOI	NZ_{ZOI}			8	0 ... 254	Nombre de zones
		$Zone^0$	DC_{ZOI}		1	0	Le segment verrouillé en octets ne suit pas
					1	1	Classe de description non associée à l'image
					6	000010	Des indices de paquet sont spécifiés
			$Pzoi^{0,0}$	Mzoi	1	0	Le segment verrouillé en octets ne suit pas.
					1	0	Les zones spécifiées sont influencées par la méthode de protection
					1	1	De multiples items sont spécifiés
					2	10	Mode indiciel
					2	xx	Izoi utilise 8 ou 16 ou 32 bits pour un entier
					1	0	Izoi est décrit dans une seule dimension
				Nzoi	8	Variable	2 ... 255 (nombre d'indices de paquet)
				$lzoi^i$	xxx Nzoi	Variable	Indice de paquet
	L_{PID}				16	0 ... $(2^{16} – 1)$	Longueur de L_{PID} + P_{ID} en octets
	P_{ID}				Variable	Variable	ID du Fichier_de_commande, URL du serveur du Fichier_de_commande, etc.); syntaxe complète fournie par le RA.

Les outils requis afin d'exécuter le découpage et le masquage de données et/ou le processus de composition en direct seront éventuellement fournis au moyen d'une connexion à l'organisme d'enregistrement et d'une importation par téléchargement à partir de cet organisme.

B.11 Flux direct à échelonnement et transcodage sécurisés

B.11.1 Résumé et motivation

Le présent paragraphe décrit une méthode permettant de fournir les services de protection de confidentialité et d'authentification du flux à codage JPEG 2000 d'une façon qui:

1) permet à une entité (éventuellement non sécurisée) de transcoder ou d'adapter en sécurité un flux JPSEC protégé sans que cette entité ait besoin de déprotéger ou de déchiffrer le contenu;

2) permet à un client de valider le fait que l'opération de transcodage a été effectuée d'une façon valide et admissible.

Un transcodage est souvent requis afin d'adapter un contenu à codage JPEG 2000 pour des clients ayant diverses capacités matérielles (p. ex. un petit format d'affichage ou des connexions réseau à bas débit) et pour des conditions de réseau variables dans le temps. La norme JPEG 2000 est particulièrement bien adaptée aux applications de transcodage en raison de ses propriétés d'échelonnabilité intrinsèques. Cependant, si l'on ne veille pas à protéger le flux à codage JPEG 2000, la propriété d'échelonnabilité peut être perdue. Par exemple, cela se produit quand la totalité du flux codé est chiffrée comme un unique fichier. Dans ce cas, le seul moyen de transcoder le flux codé et protégé consiste à le

déchiffrer puis à le transcoder ou à l'adapter. Comme le transcodeur doit déchiffrer le contenu, ce processus interrompt la sécurité de bout en bout du système.

Le système JPSEC a été conçu afin de permettre un transcodage sécurisé du contenu protégé par syntaxe JPSEC, où le terme *transcodage sécurisé* est défini comme étant un *transcodage sans déprotection (ou déchiffrement) du contenu*. C'est ce qui est réalisé avec un flux direct à échelonnement sécurisé, qui combine codage échelonnable, chiffrement et signalisation d'une façon qui autorise un transcodage sécurisé et sans complexité par un serveur distant (éventuellement non sécurisé) ou par un nœud ou serveur intermédiaire en milieu de réseau. Cela permet au système JPSEC d'obtenir les propriétés, apparemment contradictoires, du transcodage à mi-réseau et de la sécurité de bout en bout. Dans la Figure B.10 par exemple, le média est chiffré chez l'expéditeur et déchiffré seulement chez le récepteur: il reste donc chiffré à tous les points situés entre: (à gauche) un nœud à mi-réseau qui transcode en sécurité un contenu protégé pour chaque client JPSEC, et (à droite) un serveur distant non sécurisé qui transcode en sécurité et envoie en flux direct le contenu JPSEC sans le déprotéger.

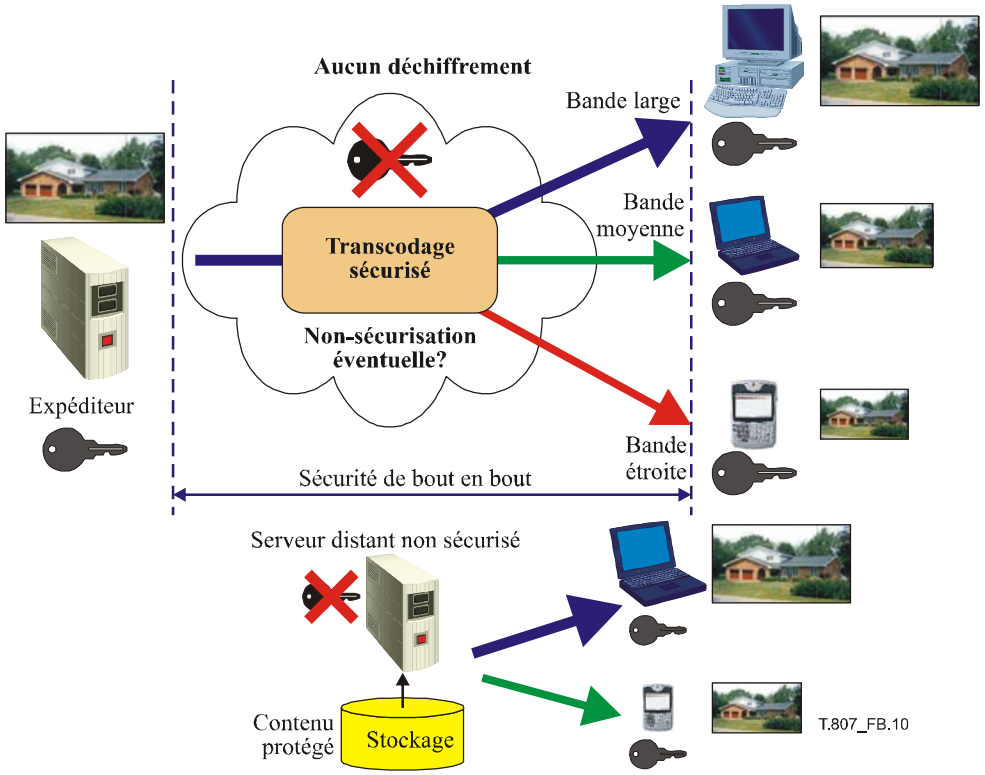


Figure B.10 – Le système JPSEC permet la sécurité de bout en bout et le transcodage à mi-réseau sécurisé

B.11.2 Description opérationnelle et deux exemples d'usage

Dans le premier exemple, le flux à codage JPEG 2000 original est dans l'ordre RLCP et l'objectif est de protéger ce flux par chiffrement et authentification tout en activant le transcodage sécurisé du flux codé et protégé en fonction de sa résolution. Comme le flux à codage JPEG 2000 original utilisait l'ordre RLCP, chaque composante de résolution est représentée par un segment de données contigu. Le chiffrement peut être effectué sur chacun des trois segments de données contigus. L'en-tête du marqueur JPSEC spécifie alors trois zones d'influence décrivant la composante de résolution, le segment de flux codé et le modèle de chiffrement servant à chaque segment. L'authentification est également effectuée sur chacun des trois segments de données, soit avant ou après chiffrement selon la fonctionnalité recherchée. Cette opération est également spécifiée dans l'en-tête de marqueur SEC au moyen du modèle d'authentification.

Afin d'exécuter un transcodage sécurisé sur le flux à codage JPSEC, un transcodeur se borne à lire et à analyser syntaxiquement l'en-tête de marqueur SEC, identifie les emplacements des segments de résolution puis conserve ou supprime les segments de données/résolutions appropriés. Noter que cette opération de transcodage correspond à une simple opération d'analyse syntaxique et qu'elle ne nécessite pas de déprotéger les données. L'authentification est effectuée par légitimation des données transcodées qui ont été reçues avec les valeurs de code MAC placées dans l'en-tête de marqueur SEC pendant le processus de protection JPSEC.

Dans le second exemple, l'objectif visé est une fois de plus de protéger le flux codé tout en autorisant le transcodage par résolution. Cependant, cet exemple est un peu plus complexe du fait que le flux à codage JPEG 2000 original est dans

l'ordre PCRL plutôt que RLCP, de sorte que les segments de données correspondant aux trois composantes de résolution ne sont pas contigus dans le flux codé original. La syntaxe JPSEC permet d'atteindre – d'un certain nombre de façons – l'objectif visé de transcodage sécurisé ou d'échelonnement par résolution. Une méthode consiste à chiffrer par paquets individuels tout en laissant les en-têtes de paquet non chiffrés. Cette méthode conserve le plus haut niveau d'échelonnabilité dans le flux mais nécessite également la très complexe opération de transcodage sécurisé parce que le transcodeur doit analyser le flux JPSEC au niveau des paquets. L'autre extrême, qui se traduit par la plus simple opération de transcodage sécurisé, consiste à réordonner les données de façon que les composantes de résolution soient une fois de plus en segments continus dont les décalages sont signalés dans l'en-tête de marqueur SEC. Cela peut être réalisé d'une façon conforme à la norme JPEG 2000 par réordonnancement des paquets JPEG 2000 de l'ordre PCRL à l'ordre RLCP puis par signalisation du nouvel ordre de progression dans le segment marqueur COD ou changement d'ordre de progression (POC, *progression order change*). Le réordonnancement des données et la transformation de protection qui en résulte sont représentés dans la Figure B.11. Une fois de plus, l'en-tête principal de marqueur SEC contient des paramètres de zone ZOI qui décrivent les paramètres correspondants, associés à l'image et associés au flux binaire, qui sont contenus dans chaque segment de données, mais cette fois dans le flux JPEG 2000 réordonné.

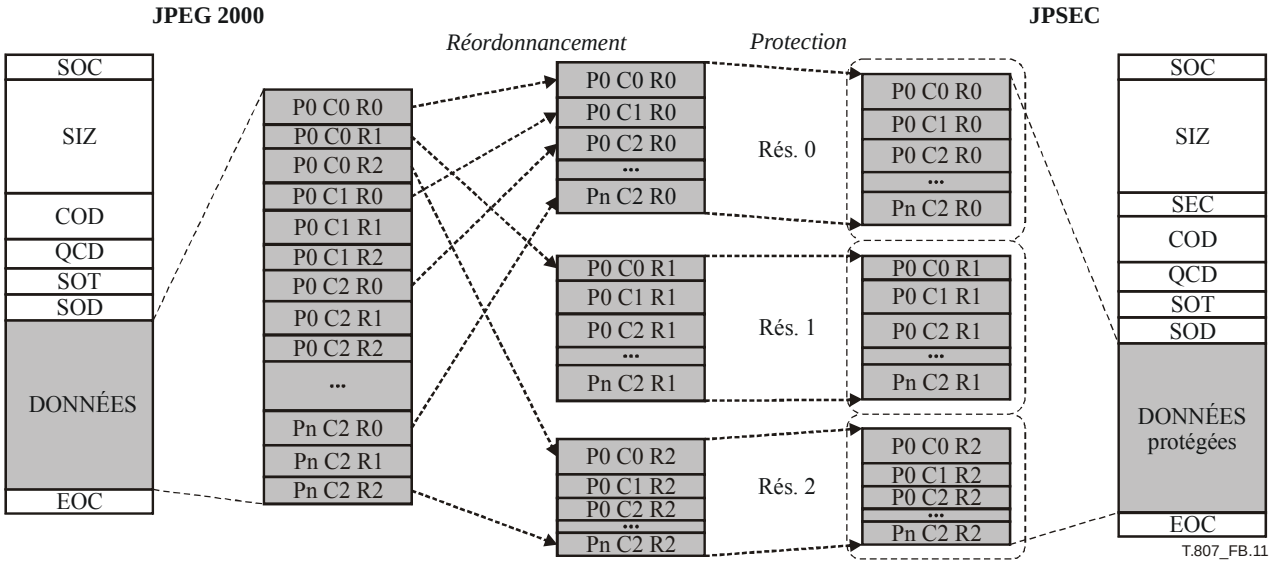


Figure B.11 – Exemple de formation d'un flux à codage JPSEC

B.11.3 Syntaxe du flux codé

La syntaxe JPSEC peut servir à créer un flux direct à échelonnement sécurisé et un système de transcodage sécurisé avec l'outil de protection de modèle. Spécifiquement, la zone d'influence (ZOI, *zone of influence*) peut être utilisée avec le modèle de déchiffrement, le domaine de traitement et la granularité afin de définir entièrement le processus de déchiffrement qu'un consommateur JPSEC autorisé devrait utiliser pour déchiffrer le flux. Par ailleurs, les paramètres de zone ZOI signalent des informations que les nœuds de transcodage peuvent utiliser afin d'exécuter le transcodage sécurisé.

Le paramètre ZOI spécifie trois zones, une pour chaque résolution et les étendues d'octet associées aux bits chiffrés pour chaque zone. La syntaxe de signalisation pour le modèle de déchiffrement de protection, le domaine de traitement et la granularité sont représentés dans le Tableau B.27. La méthode de déchiffrement est signalée avec le modèle de protection du déchiffrement. Dans ce cas, elle spécifie le chiffrement AES en mode CTR ainsi que les longueurs de bloc et de clé. Le domaine de traitement et la granularité spécifient par ailleurs comment le déchiffrement est effectué. La méthode signale que le domaine de traitement est le flux binaire proprement dit et que les en-têtes et les corps de paquet sont chiffrés. Différentes méthodes de déchiffrement peuvent être spécifiées par changement du domaine de traitement et de la granularité. Par exemple, la granularité du chiffrement peut être calculée sur des paquets individuels ou seulement sur les corps de paquet. Par ailleurs, la méthode d'authentification est spécifiée avec le même paramètre ZOI que ci-dessus, mais avec le modèle d'authentification ci-après. La syntaxe du modèle d'authentification est représentée dans le Tableau B.28 pour l'utilisation du code HMAC avec l'algorithme SHA-1 d'authentification. Evidemment, d'autres algorithmes de chiffrement JPSEC et d'autres codes MAC peuvent également être utilisés. En outre, la solution proposée peut être utilisée avec d'autres outils de signature numérique, de contrôle d'accès et de gestion des clés. Par ailleurs, une distorsion peut être associée à chaque paquet (ou à une autre zone de données) au moyen du champ de distorsion (§ 5.7.3.2) afin de permettre un flux direct et un transcodage sécurisés et optimisés en distorsion de débit (R-D) [26], [27] et [28].

Tableau B.27 – Valeurs paramétriques d'outil de protection de modèle, de domaine de traitement et de granularité

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
T_{decry}	ME_{decry}		8	0	Fanion d'émulation de marqueur de valeur NULL
	CT_{decry}		16	1	Chiffrement AES
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	CTR sans bourrage
		P_{bc}	2	0	Bourrage inutilisé pour le mode CTR
		SIZ_{bc}	8	128	La longueur de bloc est 128 bits
		KT_{bc}	Variable	*Modèle de clé*	Modèle d'informations de clé
PD			1	0_b	Un segment verrouillé en octets (BAS) ne suit pas.
			1	0_b	Hors du domaine des pixels
			1	0_b	Hors du domaine des coefficients d'ondelette
			1	0_b	Hors du domaine des coefficients d'ondelette quantifiés
			1	1_b	Traité dans le domaine du flux codé
			3	000_b	Inutilisé
G		PO	16	$0\ 0000\ 0101\ 0011\ 100_b$	Ordre de traitement: TRLCP.
		GL	8	$0000\ 1001_b$	Granularité = aire totale identifiée par la zone ZOI.
V		N_V	16	1	Une seule valeur est spécifiée
		Sv	8	16	Longueur: 16 octets.
		VL	128	*Valeur du vecteur de circonstance (sel)*	Valeur de compteur pour le mode CTR

Tableau B.28 – Valeurs paramétriques pour l'outil de protection du modèle d'authentification

Paramètre			Longueur (bits)	Valeur (dans l'ordre)	Signification déduite
T_{auth}	M_{auth}		8	0	Code MAC fondé sur un hachage
	P_{auth}	M_{HMAC}	8	1	Code HMAC
		H_{HMAC}	8	1	ID de hachage: SHA-1
		KT_{HMAC}	Variable	*Valeur de clé*	Voir modèle de clé
		SIZ_{HMAC}	16	80	Longueur de code MAC: 80 bits (tronquée à partir de 160).

B.11.4 Conclusions

Le présent paragraphe décrit le flux direct à échelonnement et le transcodage sécurisé par syntaxe JPSEC, qui autorise les deux propriétés, apparemment contradictoires, de la sécurité de bout en bout et du transcodage sécurisé aux nœuds à mi-réseau. Cela permet de transcoder le flux à codage JPSEC *sans nécessiter de déchiffrement*. Par ailleurs, cette méthode authentifie le fait que le transcodage n'a été effectué que de façon valide et admissible, ainsi que le fait qu'aucune modification non intentionnelle ou malveillante ne s'est produite à la suite d'une erreur ou d'une attaque. Cela permet à un serveur distant ou à un nœud à mi-réseau tel qu'un serveur intermédiaire (éventuellement non sécurisé) d'exécuter un transcodage sécurisé tout en autorisant un consommateur JPSEC à authentifier le fait que le contenu reçu a été transcodé d'une façon valide et admissible.

Annexe C

Interopérabilité

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

C.1 Partie 1

Un certain nombre de méthodes de protection peuvent être appliquées à un flux à codage JPEG 2000 afin de créer des flux à codage JPSEC qui restent strictement conformes à la Partie 1 de la norme JPEG 2000. L'on utilise le terme "conformité à la Partie 1" afin de désigner les flux à codage JPSEC qui ont un comportement strictement défini dans les décodeurs conformes à la Partie 1 de la norme JPEG 2000 y compris ceux qui ne sont pas informés de la syntaxe JPSEC.

Un décodeur conforme à la Partie 1 de la norme JPEG 2000 va omettre les segments marqueurs qu'il ne reconnaît pas. Un outil JPSEC, tel que l'outil JPSEC normatif pour authentification, insère dans le segment marqueur SEC les valeurs de code d'authentification de message calculées à partir des données JPEG 2000, en même temps que les paramètres qui décrivent les méthodes d'authentification particulières pouvant être utilisées par un consommateur JPSEC. Ces paramètres et valeurs indiquent à un consommateur JPSEC la façon de vérifier que le flux à codage JPSEC reçu est authentique. Remarquer que l'outil d'authentification JPSEC ne manipule pas les données JPEG 2000. Un décodeur conforme à la Partie 1 de la norme JPEG 2000, qui reçoit ce flux à codage JPSEC, va donc commencer le décodage du flux JPSEC. Il va alors omettre le segment marqueur SEC et continuer à décoder le flux JPSEC comme s'il était conforme à la Partie 1 de la norme JPEG 2000. L'outil JPSEC normatif d'authentification partage ces caractéristiques et produit donc également un flux codé conforme à la Partie 1.

La syntaxe JPSEC permet d'effectuer le chiffrement et le déchiffrement sur des flux JPEG 2000 et JPSEC. Quand le chiffrement est utilisé, les données JPEG 2000 sont évidemment modifiées. Au sens strict, la conformité à la Partie 1 n'est pas possible avec les flux chiffrés car ceux-ci feront très probablement qu'un décodeur conforme à la Partie 1 de la norme JPEG 2000 recevra des valeurs illégales. Une façon possible de résoudre ou au moins de réduire ce problème consiste à utiliser les capacités de tolérance aux erreurs du codage JPEG 2000. Avec la tolérance aux erreurs, il est possible d'avoir des flux JPSEC codés et chiffrés ayant un comportement défini dans les décodeurs conformes à la Partie 1 de la norme JPEG 2000.

La syntaxe JPSEC possède un champ paramétrique P_{sec} qui contient des paramètres de sécurité pour la totalité du flux codé. Ce champ contient un fanion F_{J2K} qui peut être réglé à 1 pour indiquer qu'un flux à codage JPSEC est décodable par les décodeurs conformes à la Partie 1 de la norme JPEG 2000. Un créateur JPSEC peut régler ce paramètre lorsqu'il applique des outils JPSEC au flux à codage JPEG 2000. Il a été mentionné qu'un créateur JPSEC pouvait accepter en entrée un flux JPSEC codé et protégé. Si un créateur JPSEC reçoit en entrée un flux codé JPSEC dont le fanion F_{J2K} est réglé afin d'indiquer la conformité à la Partie 1, puis applique un outil JPSEC qui perd la conformité à la Partie 1, ce créateur doit mettre le fanion F_{J2K} à 0.

Pour les flux JPSEC qui ne sont pas conformes à la Partie 1, il est recommandé d'utiliser l'extension de fichier .jp2s afin d'indiquer qu'un décodeur conforme à la Partie 1 de la norme JPEG 2000 peut ne pas être en mesure de décoder le flux codé et protégé.

C.2 Partie 2

L'Amendement 2 à la Partie 2 de la norme JPEG 2000 sur le segment marqueur à capacités étendues (CAP, *capabilities marker segment*) peut servir à indiquer que la syntaxe JPSEC est utilisée. Spécifiquement, la Partie 2 utilise le paramètre R_{siz} afin d'indiquer la présence d'un segment marqueur CAP qui contient un paramètre C_{cap} pouvant servir à signaler quelles parties de la norme JPEG 2000 sont utilisées dans le flux codé. On peut spécifier que la Partie 8 de la norme JPEG 2000 (JPSEC) est utilisée en activant un fanion approprié dans le paramètre C_{cap}.

Un créateur JPSEC peut donc régler le paramètre R_{siz} afin d'indiquer la présence d'un segment marqueur CAP. Il peut insérer ou éditer le segment marqueur CAP de façon à régler le paramètre C_{cap} sur l'indication que la Partie 8 est utilisée.

C.3 Protocole JPIP

C.3.1 Relation générale entre protocoles JPIP et JPSEC

La norme JPIP spécifie un protocole composé d'une série structurée d'interactions entre un client et un serveur distant au moyen de laquelle des flux codés de métadonnées de fichier d'image, de structure et d'image (partielle ou entière) peuvent être échangés d'une façon efficace en terme de communications.

Le protocole JPIP peut être adapté au moyen des diverses extensions apportées au format de fichier JPEG 2000, comme défini dans la Rec. UIT-T T.801 | ISO/CEI 15444-2, dans la Rec. UIT-T T.802 | ISO/CEI 15444-3 et dans la Rec. UIT-T T.805 | ISO/CEI 15444-6. Cependant, afin d'atteindre un simple niveau d'interactivité permettant de transférer des portions d'un unique fichier ou flux à codage JPEG 2000, ces autres capacités ne sont pas autorisées.

Des dispositions ont été incluses pour l'extension du protocole JPIP de façon à prendre en charge les actuelles normes JPEG 2000 comme la Rec. UIT-T T.802 | ISO/CEI 15444-3, la norme MPEG 2000, la Rec. UIT-T T.805 | ISO/CEI 15444-6, les formats de fichier d'image composite ainsi que les futures parties de la norme JPEG 2000 (actuellement JP3D, JPSEC et JPWL).

La syntaxe JPSEC fournit des services de sécurité pour les images JPEG 2000 et prend en charge deux types de marqueurs: SEC et INSEC. Un ou plusieurs marqueurs SEC apparaissent dans l'en-tête principal du flux binaire JPSEC. En d'autres termes, la syntaxe JPSEC consomme un flux à codage JPEG 2000, modifie l'en-tête principal JPEG 2000 de façon à former un nouvel "en-tête principal" JPSEC et modifie le flux correspondant de données JPEG 2000 de façon à former un nouveau flux de données protégées, si applicable. Des marqueurs INSEC peuvent facultativement apparaître dans la portion "données" des flux de données afin de spécifier certains paramètres de "petite longueur" ou de "région locale" par rapport au marqueur SEC. Ces marqueurs peuvent servir à compléter le marqueur SEC.

Il est observé que le protocole JPIP se situe juste au-delà de la couche de transport, alors que le protocole JPSEC est dans la couche d'application. De ce point de vue, le protocole JPIP fournit un service de transport au protocole JPSEC. C'est-à-dire que le protocole JPIP offre des outils efficaces afin de fournir des informations iconographiques entre serveurs et clients, y compris l'en-tête principal (l'ensemble des marqueurs) et le flux codé. Le présent article étudie comment le protocole JPIP peut servir à transporter un contenu JPSEC.

C.3.2 Problèmes spécifiques d'interactivité entre protocoles JPIP et JPSEC

Le présent paragraphe décrit les problèmes qu'un expéditeur et un récepteur JPIP doivent examiner afin de transporter un contenu JPSEC.

Dans le paragraphe A.3.5: "Segment de données d'en-tête principal" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, les deux types de média (flux JPP et JPT) utilisent le segment de données d'en-tête principal. Ce segment se compose d'une liste concaténée de tous les marqueurs et segments de marqueurs contenus dans l'en-tête principal, à partir du marqueur SOC. Il ne contient aucun marqueur SOT, SOD ou EOC. Cependant, l'en-tête principal du codage JPEG 2000 ne contient pas le marqueur SEC ni son segment. En conséquence, le § A.3.5 du projet final de Comité (FCD) JPIP 2.0 ne spécifie pas la prise en charge du segment marqueur SEC spécifié dans la syntaxe JPSEC. Un expéditeur et un récepteur JPIP doivent donc être modifiés afin de reconnaître le ou les segments marqueurs SEC qui apparaissent dans l'en-tête principal d'un flux à codage JPSEC.

Le paragraphe A.3.2: "Segments de données de district" de la Rec. UIT-T T.808 | ISO/CEI 15444-9 décrit sa prise en charge des données de district. Cependant, le § A.3.2 du projet final de Comité (FCD) JPIP 2.0 ne spécifie pas s'il prend en charge le marqueur INSEC et son segment tels que spécifiés dans la syntaxe JPSEC. Un expéditeur et un récepteur JPIP doivent donc être modifiés de façon à reconnaître le segment marqueur INSEC qui peut apparaître dans une portion de données d'un flux à codage JPSEC.

Dans le paragraphe A.3.3: "Segments de données d'en-tête de pavé" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, les segments de données d'en-tête de pavé apparaissent seulement dans le type de média à flux JPP. Pour les segments de données appartenant à cette classe, l'identificateur-dans-la-classe contient l'indice (à partir de 0) du pavé auquel le segment de données se rapporte. Ce segment de données se compose de marqueurs et de segments marqueurs pour le pavé n. Il ne doit pas contenir de segment marqueur SOT. L'inclusion du marqueur SOD (début de données) est facultative. Ce segment de données peut être formé à partir d'un flux codé légal, par concaténation de tous les segments marqueurs (sauf SOT et POC) dans tous les en-têtes d'élément de pavé pour le pavé n.

Dans le paragraphe A.3.4: "Segments de données de pavé" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, les segments de pavé de données ne doivent être utilisés qu'avec le type de média à flux JPT. Pour les segments de données appartenant à cette classe, l'identificateur-dans-la-classe est l'indice (à partir de 0) du pavé auquel le segment de données appartient. Chaque segment de données de pavé correspond à la chaîne d'octets formée par concaténation de tous les éléments de pavé appartenant au pavé, dans l'ordre, complets avec leurs marqueurs SOT, SOD et avec tous les autres segments marqueurs correspondants.

Comme mentionné ci-dessus, les § A.3.4 et A.3.5 de la Rec. UIT-T T.808 | ISO/CEI 15444-9 décrivent la prise en charge des données d'en-tête de pavé et d'élément de pavé. Cependant, les § A.3.4 et A.3.5 de la Rec. UIT-T T.808 | ISO/CEI 15444-9 ne spécifient pas s'ils prennent en charge les segments marqueurs SEC et INSEC. Un expéditeur et un récepteur JPIP doivent donc être modifiés de façon à reconnaître et à transporter ces segments marqueurs en même temps que les données protégées.

C.3.3 Résumé

Généralement, la syntaxe JPSEC se prête au transport par protocole JPIP. Le marqueur INSEC est utilisé dans le flux codé afin de décrire une certaine "petite" partie de données spécifiques qui est protégée par un ou des outils de sécurité. Ce marqueur rend la syntaxe JPSEC plus flexible. Afin de rendre le marqueur INSEC plus robuste, la couche de service (actuellement dénommée *JPIP*) devrait offrir le bon niveau de qualité de service ou de protection dans le marqueur INSEC et dans son segment. Afin d'atteindre cet objectif, les protocoles JPIP et JPSEC ont à résoudre certains problèmes et à vérifier leur interactivité.

C.4 Protocole JPWL

La norme JPEG 2000 sans fil ou JPWL (Rec. UIT-T T.810 | ISO/CEI 15444-11) étend les spécifications JPEG 2000 de base afin d'obtenir la transmission efficace de l'imagerie JPEG 2000 dans un environnement exposé aux erreurs. Plus spécifiquement, la norme JPWL définit un ensemble d'outils et de méthodes permettant de protéger le flux codé contre les erreurs de transmission. Il définit également la façon de décrire la sensibilité du flux codé aux erreurs de transmission et de décrire les emplacements dans le flux codé des erreurs résiduelles de transmission.

La norme JPWL traite en particulier de la protection de l'en-tête d'image, des codes de correction d'erreur directe (FEC, *forward error correcting*), de la protection adaptée à la sensibilité aux erreurs d'inégalité (UEP, *unequal error protection*), du codage conjoint source-canal, du partitionnement-entrelacement des données et du codage arithmétique robuste. Le protocole JPWL n'est pas associé à un réseau ou protocole de transport spécifique, mais fournit une solution générique pour la transmission robuste de l'imagerie JPEG 2000 sur les réseaux exposés aux erreurs.

Les principales fonctionnalités du protocole JPWL sont les suivantes:

- protéger le flux codé contre les erreurs de transmission;
- décrire le degré de sensibilité de différentes parties du flux codé aux erreurs de transmission;
- décrire les emplacements des erreurs résiduelles dans le flux codé.

Le protocole JPWL définit quatre segments marqueurs: capacité de protection contre les erreurs (EPC, *error protection capability*), bloc de protection contre les erreurs (EPB, *error protection block*), descripteur de sensibilité aux erreurs (ESD, *error sensitivity descriptor*) et descripteur d'erreur résiduelle (RED, *residual error descriptor*).

Le segment marqueur EPC indique que des outils normatifs et informatifs JPWL sont utilisés dans le flux codé. Plus spécifiquement, le marqueur EPC signale si les trois autres segments marqueurs normatifs, définis par JPWL, à savoir le descripteur de sensibilité aux erreurs (ESD), le descripteur d'erreur résiduelle (RED) et le bloc de protection contre les erreurs (EPB) sont présents dans le flux codé. Par ailleurs, le segment marqueur EPC signale l'utilisation d'outils informatifs qui ont déjà été enregistrés auprès de l'organisme d'enregistrement JPWL. Le marqueur EPC est obligatoire dans un flux codé JPWL.

La fonction principale du segment marqueur EPB est de protéger l'en-tête principal et l'en-tête d'élément de pavé. Cependant, il peut également servir à protéger le reste du flux codé. Le segment marqueur EPB contient des informations sur les paramètres de protection contre les erreurs et sur les données de redondance servant à protéger le flux codé contre les erreurs.

Le segment marqueur ESD contient des informations sur la sensibilité du flux codé aux erreurs. Ces informations peuvent être exploitées lors de l'application d'une technique de protection adaptée à la sensibilité aux erreurs d'inégalité (UEP). En termes plus directs, des codes plus puissants servent à protéger la portion sensible du flux codé. Ces informations peuvent également être utilisées pour des retransmissions sélectives. Finalement, les informations transportées dans le segment ESD pourraient également être utilisées pour d'autres applications que le protocole JPWL, comme le transcodage efficace de débit ou la prélecture intelligente.

Le segment marqueur RED signale la présence d'erreurs résiduelles dans le flux codé. En fait, un décodeur JPWL peut ne pas arriver à corriger toutes les erreurs d'un flux codé. Le segment marqueur RED permet de signaler l'emplacement de telles erreurs résiduelles. Ces informations peuvent alors être exploitées par un décodeur JPEG 2000 afin de mieux faire face aux erreurs. P. ex., le décodeur pourrait demander une retransmission, masquer les erreurs ou rejeter les informations corrompues.

C.4.1 Relation générale entre JPWL et JPSEC

La combinaison des protocoles JPWL et JPSEC est requise chaque fois que des images JPEG 2000 ont besoin d'être sécurisées et transmises dans un canal sans fil exposé aux erreurs.

Du côté émetteur, la sensibilité aux erreurs JPWL est normalement produite pendant le codage JPEG 2000. Les outils JPSEC sont alors appliqués au flux codé afin de le sécuriser. Finalement les outils de codage JPWL servent à rendre le flux codé plus résistant aux erreurs de transmission.

Du côté récepteur, les outils de décodage JPWL sont d'abord appliqués afin de corriger d'éventuelles erreurs de transmission. Pendant cette étape, l'outil JPWL peut également produire des informations relatives aux erreurs résiduelles. Finalement, les outils JPSEC sont appliqués afin d'exécuter les services de sécurité sélectionnés.

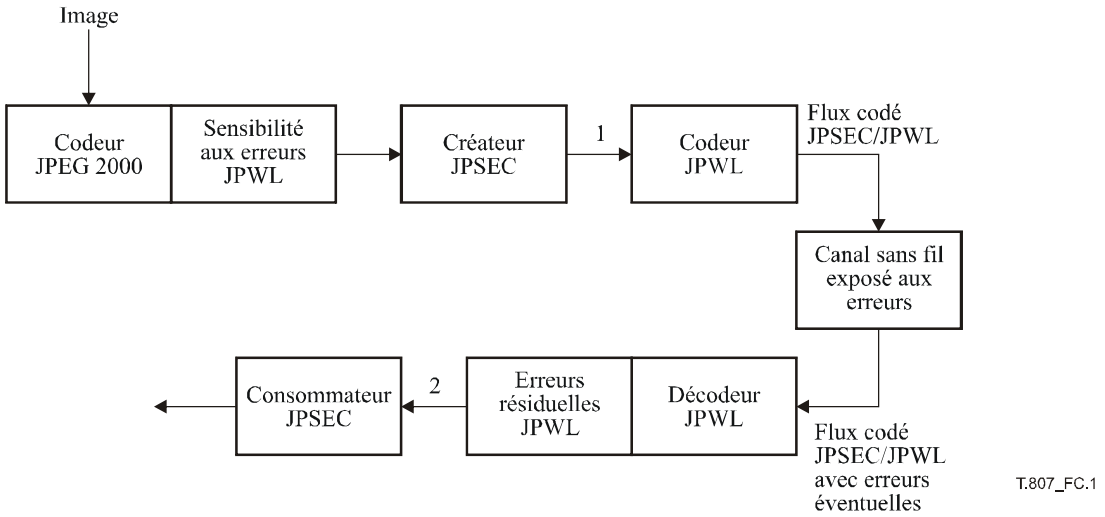


Figure C.1 – Combinaison typique des protocoles JPWL et JPSEC

C.4.2 Problèmes spécifiques d'interopérabilité entre protocoles JPWL et JPSEC

Un certain nombre de problèmes doivent être considérés quant à l'interopérabilité entre les protocoles JPWL et JPSEC, comme détaillé ci-après:

1) capacité JPWL de protection contre les erreurs (EPC): la présence de ce segment marqueur va affecter les étendues d'octet. Noter que ce segment marqueur est obligatoire dans un flux codé JPWL.
2) bloc JPWL de protection contre les erreurs (EPB): ce segment marqueur est normalement ajouté en dernière étape dans l'émetteur et supprimé en première étape dans le récepteur. En principe, il ne devrait pas affecter les flux JPSEC.
3) descripteur JPWL de sensibilité aux erreurs (ESD): ce segment marqueur est normalement ajouté pendant le codage conforme à la Partie 1 de la norme JPEG 2000, auquel cas il sera transparent aux opérations JPSEC subséquentes. Cependant, le protocole JPSEC pourrait affecter défavorablement l'utilisation du marqueur ESD dans le protocole JPWL. En particulier, JPSEC ne devrait pas modifier les étendues d'octet chaque fois que le marqueur ESD utilise des étendues d'octet. En outre, les opérations JPSEC ne devraient pas affecter les valeurs de distorsion; sinon les informations transportées par le marqueur ESD deviendraient inapplicables. Dans ce dernier cas, le créateur JPSEC a la possibilité de supprimer le segment marqueur ESD.
4) descripteur JPWL d'erreur résiduelle (RED): ce segment marqueur peut être inséré après le décodage JPWL. Il peut donc affecter les étendues d'octet JPSEC. Il peut également influencer les techniques d'authentification JPSEC. En cas de flux codé corrompu, les informations du marqueur RED peuvent être utiles à un consommateur JPSEC afin de les traiter de façon appropriée.
5) marqueur SEC JPSEC: la présence de ce segment marqueur va affecter les étendues d'octet. Noter que ce segment marqueur est obligatoire dans un flux à codage JPSEC.
6) marqueur INSEC JPSEC: la présence de ce segment marqueur va affecter les étendues d'octet. Noter que ce segment marqueur apparaît dans les données du flux codé.

S'il n'y a aucune erreur résiduelle, le codeur et le décodeur JPWL devraient théoriquement être transparents. En d'autres termes, les flux des points 1 et 2 dans la Figure précédente devraient dans ce cas être strictement identiques.

A titre de recommandation générale, quand la syntaxe JPSEC est utilisée en combinaison avec la syntaxe JPWL, il est préférable que JPSEC utilise des étendues d'octet commençant après le marqueur SOD (début de données) afin de minimiser les problèmes d'étendues d'octet. En outre, il est préférable d'interdire la présence de segments marqueurs JPWL dans l'en-tête principal et d'éviter leur présence dans les en-têtes d'élément de pavé.

Annexe D

Déclarations relatives aux brevets

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

NOTE – L'annexe D est propre à l'ISO/CEI. Les compagnies qui soumettent des déclarations de brevet à l'UIT relatives au texte présent sont inscrites dans la base UIT des déclarations IPR. Voir http://itu.int/ITU-T/ipr/

L'Organisation internationale de normalisation (ISO, *International Organization for Standardization*) et la Commission électrotechnique internationale (CEI) attirent l'attention sur le fait qu'il est revendiqué que la conformité à la présente partie de l'ISO/CEI 15444 peut impliquer l'utilisation de brevets.

L'ISO et la CEI ne prennent aucune position concernant la preuve, la validité et le domaine d'application de ces droits de brevet ou de propriété industrielle.

Les détenteurs de ces droits de brevet ou de propriété industrielle ont assuré l'ISO et la CEI qu'ils étaient disposés à négocier des licences à des termes et conditions raisonnables et non discriminatoires avec des requérants dans le monde entier. A cet égard, les déclarations des détenteurs de ces droits de brevet sont enregistrées auprès de l'ISO et de la CEI. Des renseignements peuvent être obtenus auprès des compagnies énumérées ci-dessous.

L'attention est attirée sur la possibilité que certains des éléments de la présente partie de l'ISO/CEI 15444 puissent faire l'objet de droits de brevet ou de propriété industrielle autres que ceux qui sont identifiés dans la présente annexe. L'ISO et la CEI ne doivent pas être tenues responsables de l'identification de tout ou partie de tels droits de brevet ou de propriété industrielle.

Tableau D.1 – Liste de déclarations

Numéro	Entité soumissionnaire
1	Canon Inc.
2	Columbia University
3	EMITALL Surveillance
4	HP
5	Institute for Infocomm Research
6	MediaLive
7	New Jersey Institute of Technology

BIBLIOGRAPHIE

[1] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

ISO/CEI 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

[2] ISO/CEI 9796-2:2002, *Technologies de l'information – Techniques de sécurité – Schémas de signature numérique rétablissant le message – Partie 2: Mécanismes basés sur une factorisation entière.*

[3] ISO/CEI 9797-1:1999, *Technologies de l'information – Techniques de sécurité – Codes d'authentification de message (MAC) – Partie 1: Mécanismes utilisant un cryptogramme bloc.*

[4] ISO/CEI 9798-1:1997, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 1: Généralités.*

[5] ISO/CEI 10118-1:2000, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 1: Généralités.*

[6] ISO/CEI 10118-2:2000, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n bits.*

[7] ISO/CEI 10118-3:2004, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 3: Fonctions de brouillage dédiées.*

[8] ISO/CEI 10118-4:1998, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 4: Fonctions de brouillage utilisant l'arithmétique modulaire.*

[9] ISO/CEI 11770-1:1996, *Technologies de l'information – Techniques de sécurité – Partie 1: Cadre général.*

[10] ISO/CEI 11770-2:1996, *Technologies de l'information – Techniques de sécurité – Gestion de clés – Partie 2: Mécanismes utilisant des techniques symétriques.*

[11] ISO/CEI 11770-3:1999, *Technologies de l'information – Techniques de sécurité – Gestion de clés – Partie 3: Mécanismes utilisant des techniques asymétriques.*

[12] ISO/CEI 13335-1:2004, *Technologies de l'information – Techniques de sécurité – Gestion de la sécurité des technologies de l'information et des communications – Partie 1: Concepts et modèles pour la sécurité des technologies de l'information et des communications.*

[13] ISO/CEI TR 13335-4:2000, *Technologies de l'information – Lignes directrices pour la gestion de la sécurité IT – Partie 4: Sélection de sauvegardes.*

[14] ISO/CEI 14888-1:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 1: Généralités.*

[15] ISO/CEI 14888-3:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 3: Mécanismes fondés sur un certificat.*

[16] ISO/CEI 15946-2:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques: Partie 2 – Signatures digitales.*

[17] ISO/CEI 15946-3:2002, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques: Partie 3 – Etablissement de clé.*

[18] ISO/CEI 15946-4:2004, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques: Partie 4 – Signatures digitales offrant un message de recouvrement.*

[19] ISO/CEI 18033-2:2006, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 2: Chiffres asymétriques.*

[20] ISO/CEI 18033-3:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 3: Chiffrement par blocs.*

[21] ISO/CEI 18033-4:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 4: Chiffrements en flot.*

[22] DWORKIN (Morris): Recommendation for Block Cipher Modes of Operation, Methods and Techniques (Recommandation sur les modes d'opération à chiffrement par blocs – Méthodes et techniques), *NIST Special Publication 800-38A*.

[23] GROSBOIS (R.), GERBELOT (P)., EBRAHIMI (T.): Authentication and access control in the JPEG 2000 compressed domain *(Authentification et contrôle d'accès dans le domaine JPEG 2000 comprimé)*, *In Proc. of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV*, San Diego, 29 juillet-3 août 2001.

[24] http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html, Java Cryptography Architecture API Specification and reference (Spécification et référence de l'interface API avec l'architecture cryptographique en langage Java).

[25] RIVEST (R.L.), SHAMIR (A.), ADLEMAN (L.M.): A method for obtaining digital signatures and public-key cryptosystems, *(Méthode d'obtention de signatures numériques et systèmes cryptographiques à clé publique)*, *Communications of the ACM (2) 21*, 1978, Page(s): 120-126.

[26] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Video Streaming for Wireless Networks, *(Flux vidéo en direct sécurisés et modulables pour réseaux sans fil) IEEE Inter. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, March 2001. Also available at www.hpl.hp.com/personal/John_Apostolopoulos/papers/SecureScalableStreaming_ICASSP01.pdf.

[27] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming Enabling Transcoding Without Decryption, *(Flux direct à échelonnement sécurisé permettant le transcodage sans déchiffrement)*, *IEEE Inter. Conf. on Image Processing (ICIP)*, http://lib.hpl.hp.com/techpubs/2001/HPL 2001 320.html Sept. 2001.

[28] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming and Secure Transcoding with JPEG 2000, *(Flux direct à échelonnement sécurisé et transcodage sécurisé avec JPEG 2000)*, *IEEE Inter. Conf. on Image Processing (ICIP)*, Sept. 2003. http://lib.hpl.hp.com/techpubs/2003/HPL-2003-117.html.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	**Terminaux des services télématiques**
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2007